DFIR Case Studies

Guidelines for the Frontliners

Setthawhut Saennam

MFEC

18 August 2023

Disclaimer

Any views or opinions presented in this presentation are solely those of the author and do not necessarily represent those of the employer.

About me

- Information Security Consultant and CSOC Team Lead
- Experienced in DFIR, CTI, TH, ITSM, and ISMS
- Technical writer and public speaker

GIAC Certified Incident Handler (GCIH)
Global Information Assurance Certification...

GIAC Certified Forensic Analyst (GCFA)
Global Information Assurance Certification...

GIAC Certified Forensic Examiner (GCFE)
Global Information Assurance Certification...

[REDACTED]

Purposes of this presentation

- Review current standards, frameworks, and guidelines
- Discuss theory and practice in the real world
- Sharing of mistakes and lessons learned

Topics

- DFIR review
  - Processes, techniques, limitations, and workarounds
  - Cooperation between CSIRT and LE
- Case studies
  - Case #1: Live incident response
  - Case #2: Investigating banking trojan
- Q&A

What is DFIR?

Digital Forensics and Incident Response (DFIR) is a field within cybersecurity that focuses on the identification, investigation, and remediation of cyberattacks.

DFIR has two main components:

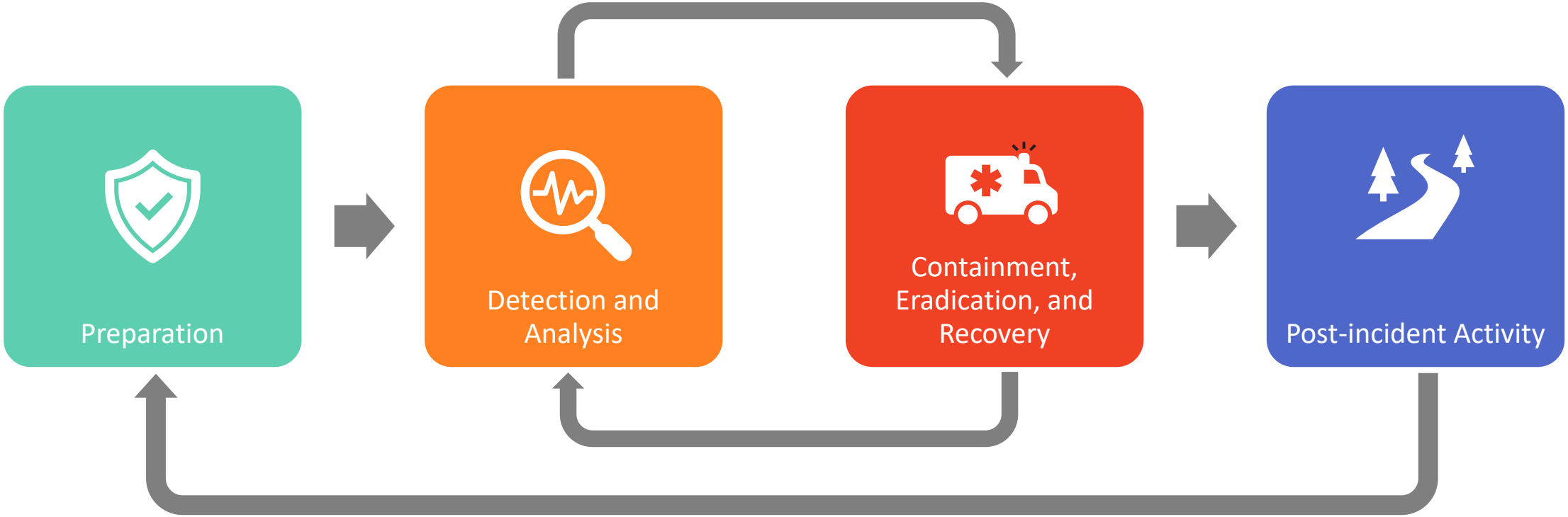
- **Digital Forensics:** A subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind the activity.
- **Incident Response:** The overarching process that an organization will follow in order to prepare for, detect, contain, and recover.

CrowdStrike - Digital Forensics and Incident Response (DFIR)
https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/

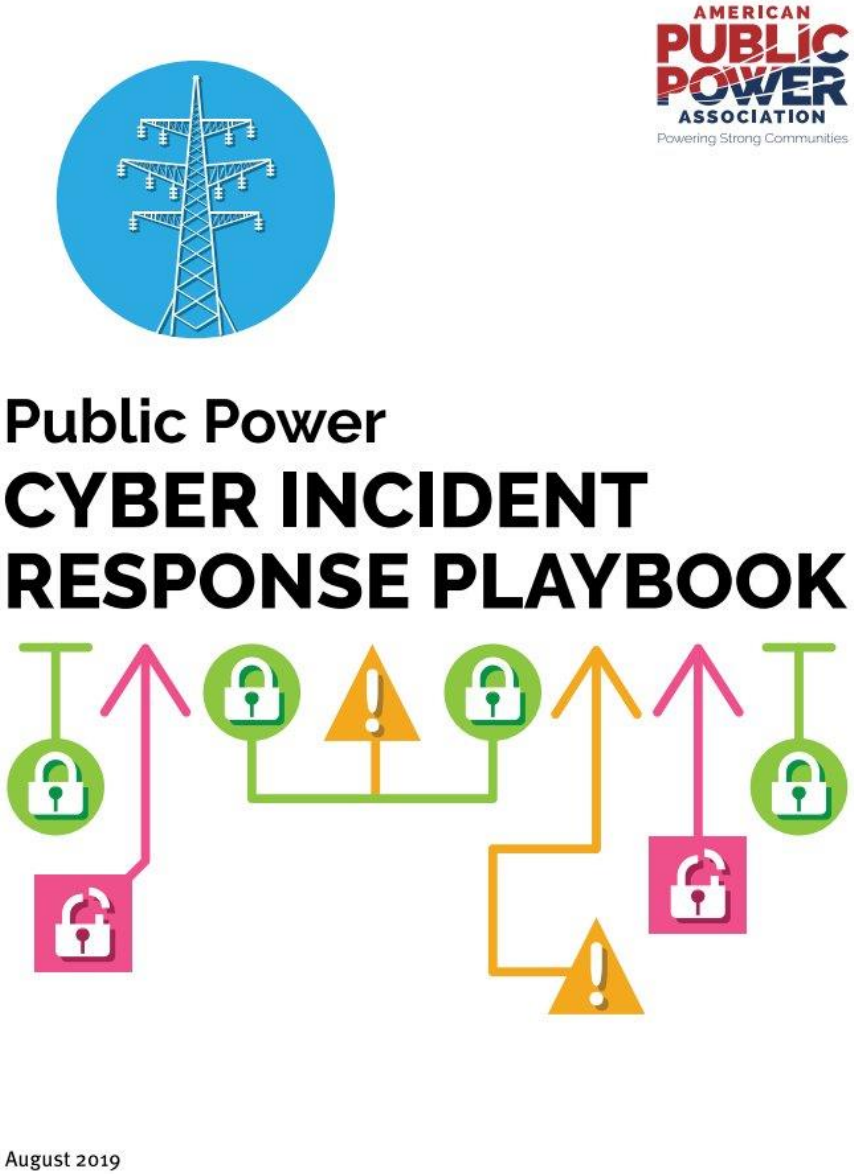
Comparison of incident response frameworks

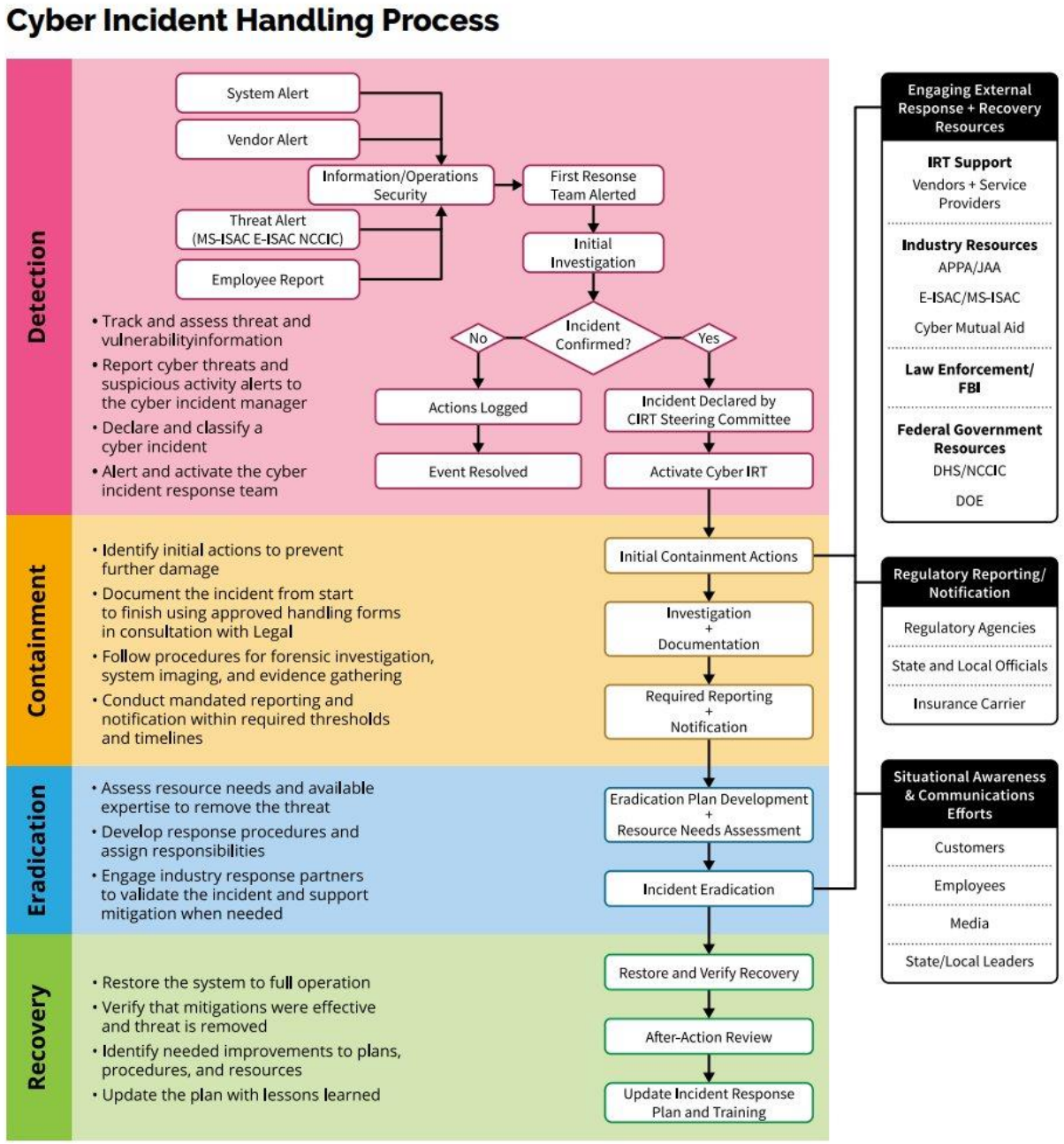
Incident response step	NIST SP 800-61r2	SANS IR	ISO/IEC 27035:2023
Planning	Preparation	Preparation	Plan and Prepare
Preparation			
Detection	Detection and Analysis	Identification	Detect and Report
Reporting			
Assessment			Assess and Decide
Decision			
Containment	Containment, Eradication, and Recovery	Containment	Respond
Eradication		Eradication	
Recovery		Recovery	
Lesson learned	Post-incident Activity	Lesson learned	Learn lessons

NIST incident response life cycle



NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf





https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

ATT&CK, D3FEND, and RE&CT

- MITRE ATT&CK
  - Stands for Adversarial Tactics, Techniques, and Common Knowledge.
- MITRE D3FEND
  - Stands for Detection, Denial, and Disruption Framework Empowering Network Defense.
- ATC RE&CT
  - Based on the MITRE's ATT&CK framework.
  - Designed for accumulating, describing and categorizing actionable Incident Response techniques.

FourCore - ATT&CK + D3FEND = D.E.A.T.H
https://fourcore.io/blogs/mitre-attack-mitre-defend-detection-engineering-threat-hunting

ATT&CK Matrix for Enterprise

layout: flat | show sub-techniques | hide sub-techniques

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (39 techniques)	Credential Access (15 techniques)	Discovery (27 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Indirect Command Execution		Process Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Masquerading (6)		Query Registry		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Remote System Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
								System Owner/User Discovery					
								System Service Discovery					
								System Time Discovery					
								Virtualization/Sandbox					

MITRE ATT&CK
https://attack.mitre.org/

DEFEND™

A knowledge graph of cybersecurity countermeasures

0.12.0-BETA-2

ATT&CK Lookup | Search D3FEND's 521 Artifacts | D3FEND Lookup

Model	– Harden				– Detect							– Isolate		– Deceive		– Evict		
+	**Application Hardening**	**Credential Hardening**	**Message Hardening**	**Platform Hardening**	**File Analysis**	**Identifier Analysis**	**Message Analysis**	**Network Traffic Analysis**	**Platform Monitoring**	**Process Analysis**	**User Behavior Analysis**	**Execution Isolation**	**Network Isolation**	**Decoy Environment**	**Decoy Object**	**Credential Eviction**	**File Eviction**	**Process Eviction**
	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	File Removal	Process Suspension
	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	Email Removal	Process Termination
	Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis		Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet	Decoy Persona	Credential Revoking		
	Pointer Authentication	Credential Rotation		File Encryption	File Hashing	Domain Name Reputation Analysis		Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	IO Port Restriction	Forward Resolution Domain Denylisting		Decoy Public Release			
	Process Segment Execution Prevention	Credential Transmission Scoping		Local File Permissions		File Hash Reputation Analysis		Passive Certificate Analysis	System Firmware Verification	Process Self-Modification Detection	Job Function Access Pattern Analysis	Kernel-based Process Isolation	Hierarchical Domain Denylisting		Decoy Session Token			
	Segment Address Offset Randomization	Domain Trust Policy		RF Shielding		IP Reputation Analysis		Client-server Payload Profiling	Operating System Monitoring	Process Spawn Analysis	Local Account Monitoring	Mandatory Access Control	Homoglyph Denylisting		Decoy User Credential			
	Stack Frame Canary Validation	Multi-factor Authentication		Software Update		URL Reputation Analysis		Connection Attempt Analysis	Endpoint Health Beacon	Process Lineage Analysis	Resource Access Pattern Analysis	System Call Filtering	Forward Resolution IP Denylisting					
		One-time Password		System Configuration Permissions		URL Analysis		DNS Traffic Analysis	Input Device Analysis	Script Execution Analysis	Session Duration Analysis		Reverse Resolution IP Denylisting					
		Strong Password Policy		TPM Boot Integrity				File Carving	Memory Boundary Tracking	Shadow Stack Comparisons	User Data Transfer Analysis		Encrypted Tunnels					
		User Account Permissions						Inbound Session Volume Analysis	Scheduled Job				Network Traffic Filtering					

MITRE D3FEND

https://d3fend.mitre.org/

RE&CT

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned
Practice	List victims of security alert*	Patch vulnerability*	**Report incident to external companies**	Reinstall host from golden image*	**Develop incident report**
Take trainings	List host vulnerabilities*	**Block external IP address**	Remove rogue network device*	Restore data from backup*	**Conduct lessons learned exercise**
Raise personnel awareness	**Put compromised accounts on monitoring**	**Block internal IP address**	**Delete email message**	**Unblock blocked IP**	
Make personnel report suspicious activity	List hosts communicated with internal domain*	**Block external domain**	Remove file*	**Unblock blocked domain**	
Set up relevant data collection*	List hosts communicated with internal IP*	**Block internal domain**	Remove registry key*	**Unblock blocked URL**	
Set up a centralized long-term log storage*	List hosts communicated with internal URL*	**Block external URL**	Remove service*	Unblock blocked port*	
Develop communication map*	Analyse domain name*	**Block internal URL**	**Revoke authentication credentials**	Unblock blocked user*	
Make sure there are backups*	Analyse IP*	**Block port external communication**	Remove user account*	**Unblock domain on email**	
Get network architecture map*	Analyse URI*	**Block port internal communication**		**Unblock sender on email**	
Get access control matrix*	List hosts communicated by port*	**Block user external communication**		**Restore quarantined email message**	
Develop assets knowledge base*	List hosts connected to VPN*	**Block user internal communication**		Restore quarantined file*	

ATC RE&CT
https://atc-project.github.io/atc-react/

PUBLICATIONS

Digital Investigation Techniques: A NIST Scientific Foundation Review

Published: November 21, 2022

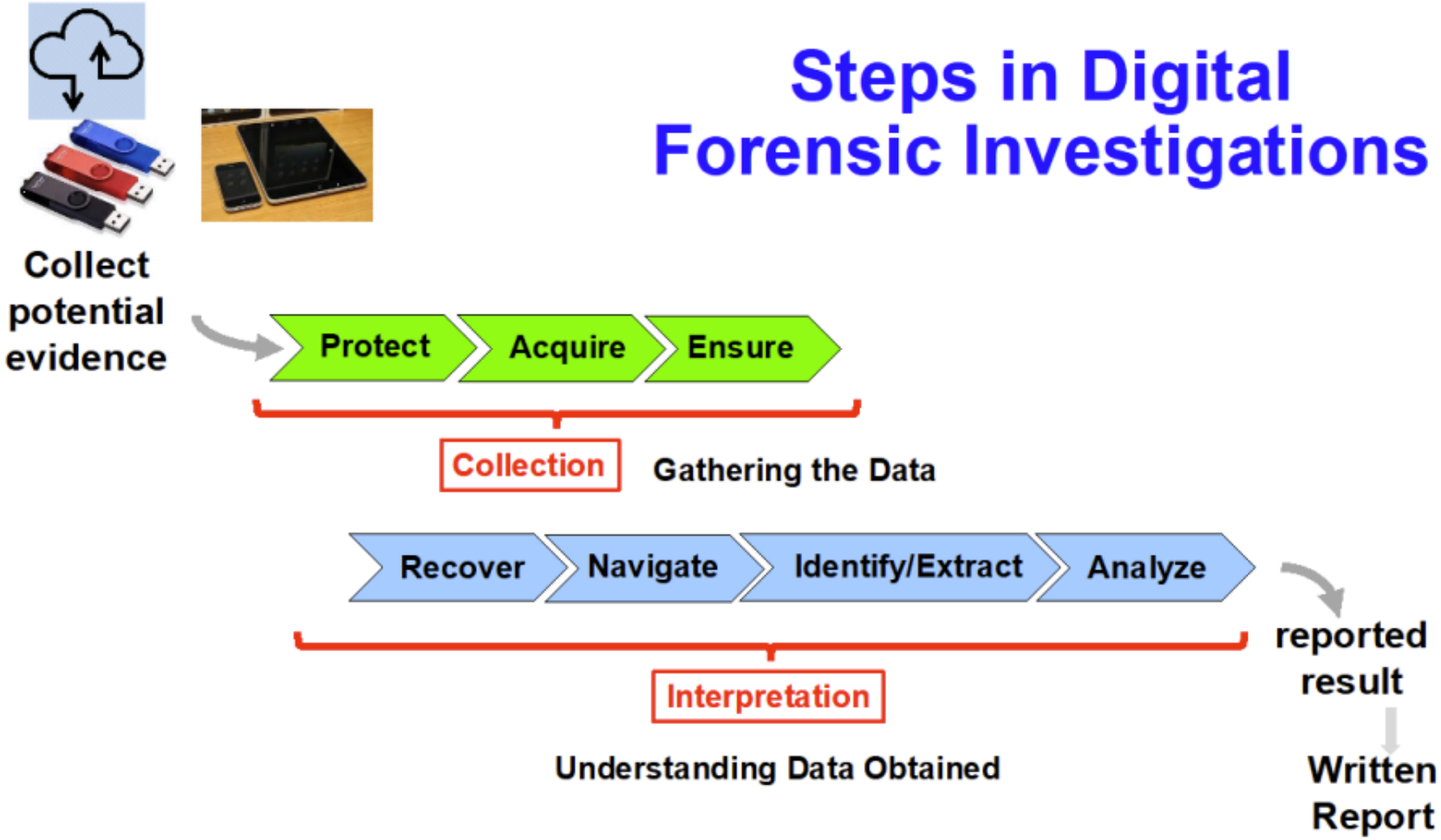
Author(s)
James R. Lyle, **Barbara Guttman**, **John Butler**, **Kelly Sauerwein**, **Christina Reed**, **Corrine Lloyd**

Abstract
This document is an assessment of the scientific foundations of digital forensics. We examined descriptions of digital investigation techniques from peer-reviewed sources, academic and classroom materials, technical guidance from professional organizations, and independently published sources. Digital investigation techniques are based on established computer science methods and when used appropriately are considered reliable. The process of evaluating, for example, the contents of a computer hard drive does not create information that was not there before the investigation started. However, because the field is rapidly changing there are limitations that practitioners and stakeholders need to be aware of: (1) as with any crime scene not all evidence may be discovered; (2) when recovering deleted files, the results may include extraneous material; (3) examiners need to understand that as software (operating systems and applications) are revised the meaning and significance of digital artifacts created by the software can change over time.

Citation: NIST Interagency/Internal Report (NISTIR) - 8354

https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review

Steps in Digital Forensic Investigations



NISTIR 8354 - Digital Investigation Techniques: A NIST Scientific Foundation Review
https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review

Steps in digital forensic investigations

- Collection
  - Protect original data from unintended modification
  - Acquire digital data
  - Ensure the integrity of acquired data
- Interpretation
  - Recover deleted data
  - Navigate and examine the acquired data
  - Identify and extract data artifacts
  - Analyze the artifacts

NISTIR 8354 - Digital Investigation Techniques: A NIST Scientific Foundation Review
https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review

Ransomware Criminals Targeted in Ukrainian Police Raids
https://www.youtube.com/watch?v=ANL1Kz3MuGk

Evidence handling

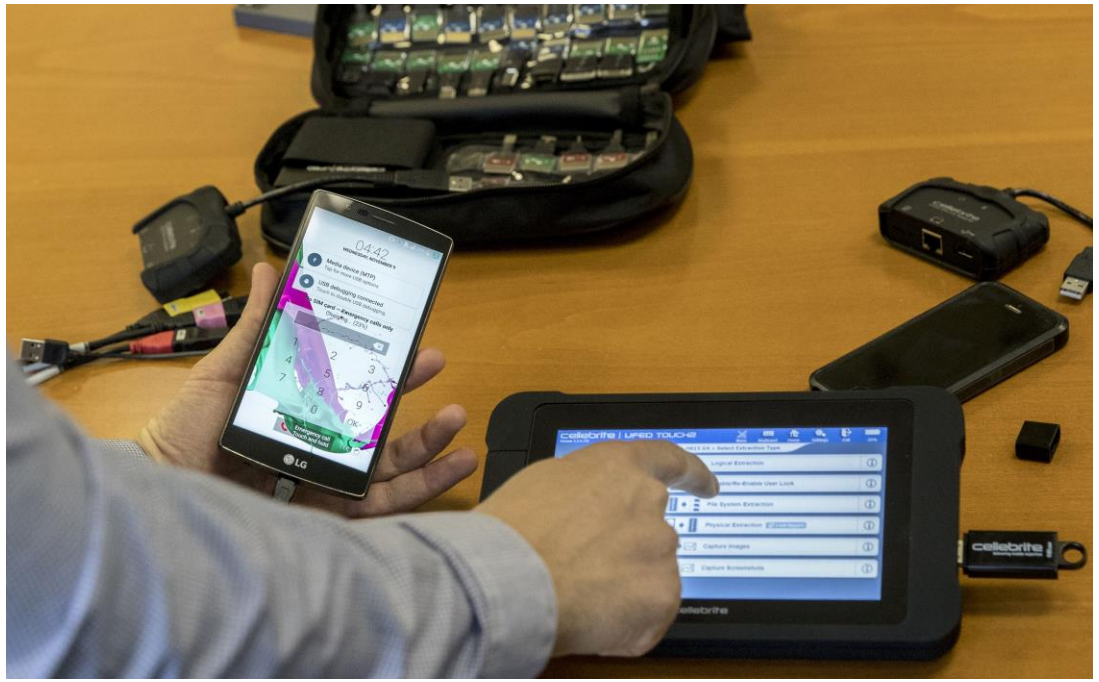
- Evidence preservation
  - Identify affected activities when acquiring data on a running system
  - Determine whether to use a write blocker or loading tool into memory
- Evidence acquisition
  - Storage device, mobile device, embedded device, etc.
  - Remote and cloud acquisition
  - Data integrity verification
- Evidence documentation
  - Technical/Legal/Operational limitations
  - Chain of custody

Evidence preservation

Photos: https://lifars.com/2021/05/how-to-acquire-digital-evidence-for-forensic-investigation/

Photo: https://www.forensicstore.com/product/black-hole-faraday-bag-kit/

Evidence acquisition



Photos: https://en.wikipedia.org/wiki/Forensic_disk_controller

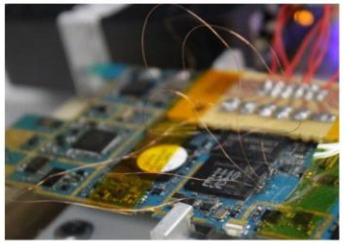
Photo: https://mashable.com/article/used-iphone-hacking-tools-sale-ebay

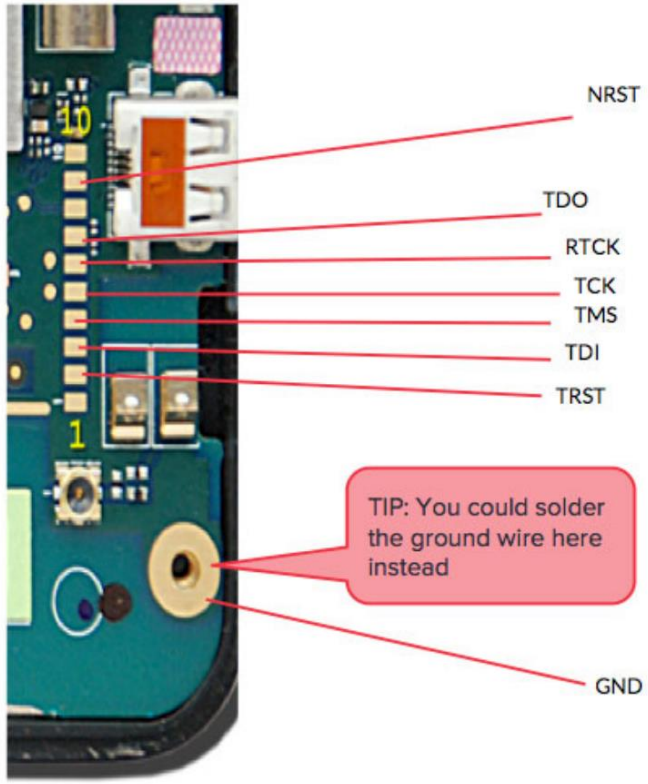
Evidence acquisition (cont.)

- Level 1
  - Manual Extraction

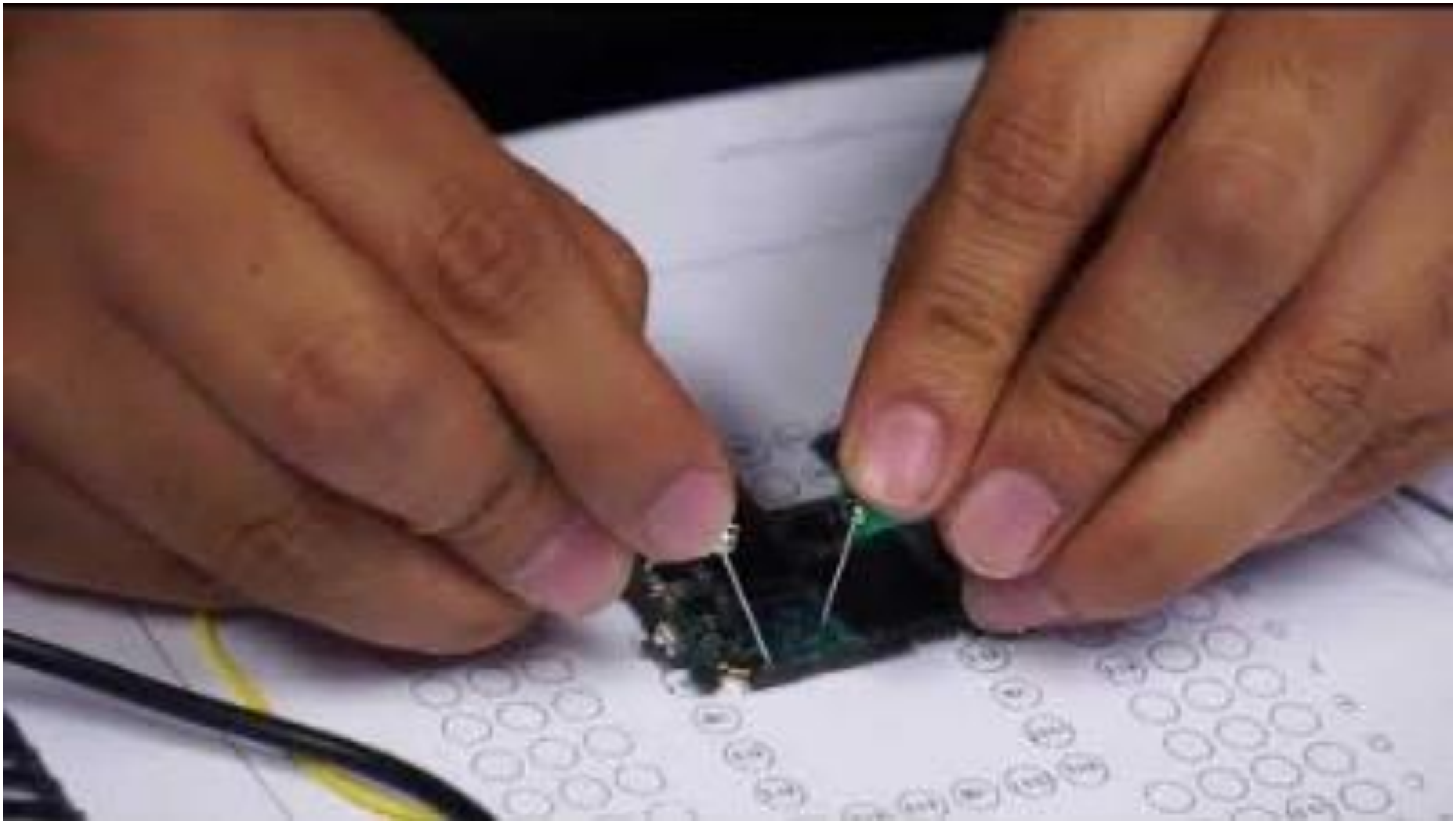
- Level 2 – 3
  - Logical Extraction
  - Physical Extraction

- Level 4-5
  - JTAG
  - Chip-Off





NIST – JTAG & Chip-off
- https://www.nist.gov/system/files/documents/2020/08/21/CFTT%20-%20JTAG%20and%20Chip-Off%202019.pdf
- https://www.nist.gov/system/files/documents/2020/08/21/JTAG%20and%20Chip-Off%20Data%20Analysis%20and%20Testing_AAFS_2020.pdf



Chip-Off ISP JTAG Training
https://www.youtube.com/watch?v=Vv-CYwwGpuE

Evidence documentation

Photos: https://www.omnigo.com/blog/3-risk-factors-that-could-break-the-chain-of-custody

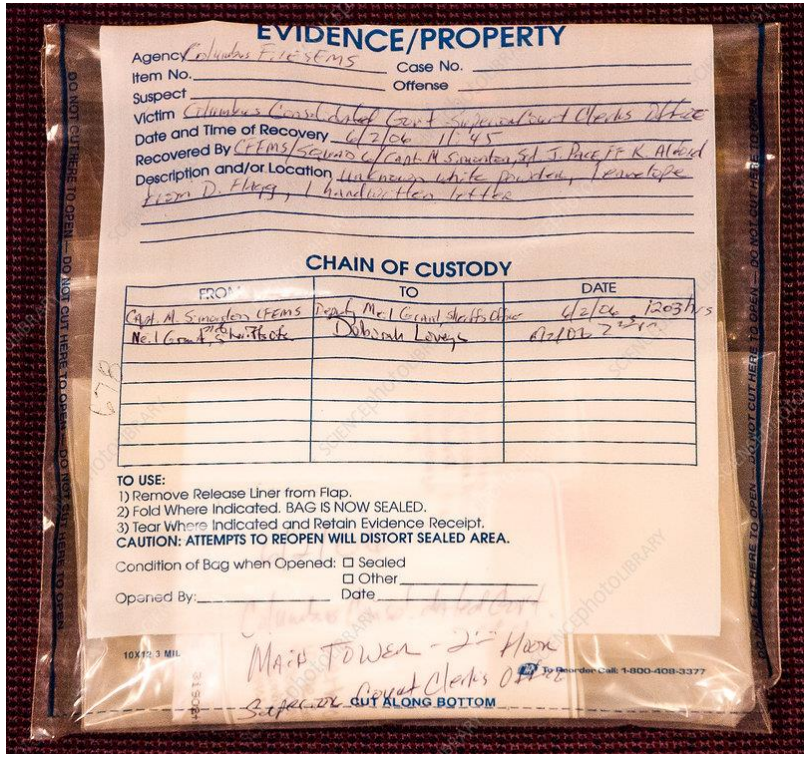
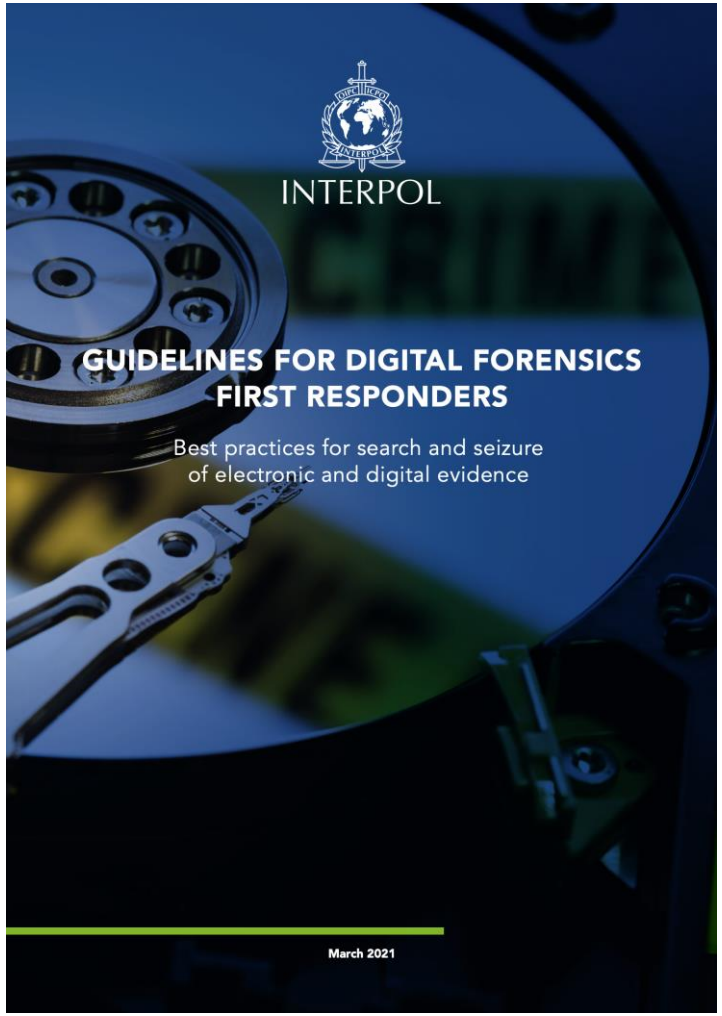


Photo: https://www.sciencephoto.com/media/1148797/view/chain-of-custody-evidence-container

Guidelines for first responders



Topics

- Search and seizure preparation and execution
- On-scene digital evidence collection and handling
- Technical considerations
- Procedures
  - Server, PC, laptop, external storage
  - Smartphone, smartwatch, tablet, SIM card, memory card
  - Digital camera, dash camera, GPS
  - IoT devices (smart TV, smart speaker, home kit)
  - Gaming console
  - Drone
  - CCTV, IP camera
  - Virtual assets device (cryptocurrency wallet)
  - Automotive vehicle

Interpol - Guidelines for Digital Forensics First Responders
https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

Guidelines for first responders (cont.)

2.2. The final destination of the evidence

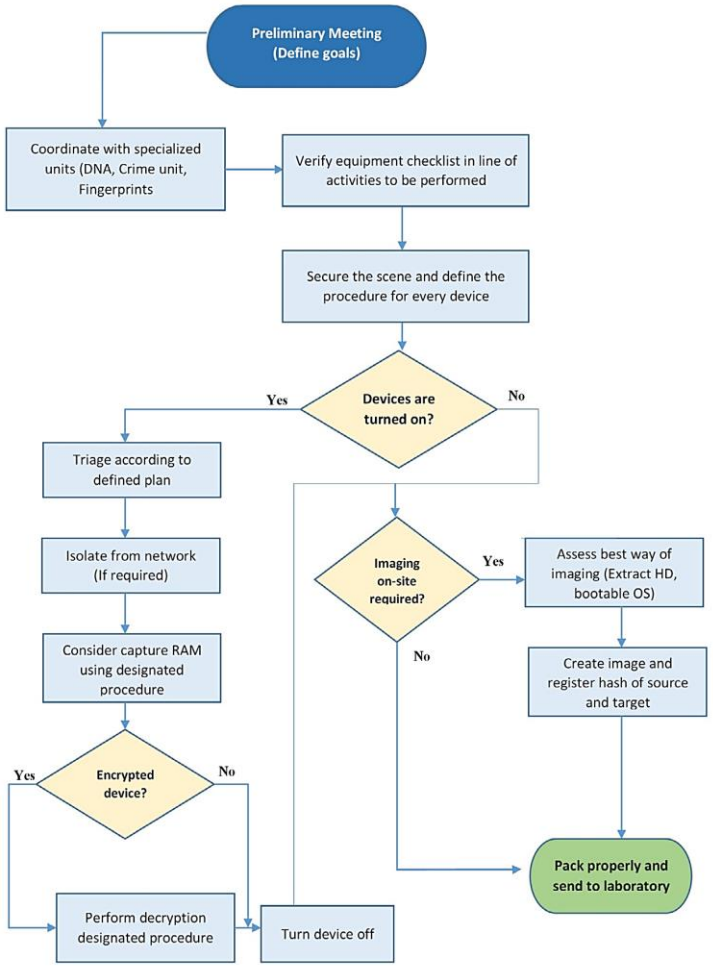


Figure 1: Flowchart showing the procedure and planning phase

Volatile Fragment	Windows tools	Linux tools
RAM content	Dumpit, Winen, Mdd, FTK Imager	dd, fmem
Routing table, ARP cache, Kernel statistics	Route PRINT, arp –a, netstat	netstat –r –n route arp -a
DNS cache	Ipconfig/displaydns	mdc dumpdb (if installed)
List of running processes	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
Active network connections		netstat –a, ifconfig
Programs and services using the network	sc queryex, netstat -ab	netstat -tunp
Open files	Handle, PsFile, Openfiles, net file	lsof, fuser
Network shares	Net share, Dumpsec	showmount –e, showmount –a smbclient -L
Open ports	OpenPorts, ports, netstat -an	netstat –an, lsof
Connected users	Psloggedon, whoami, ntlast, netusers /l	w, who –T, last
Encrypted archives	Manage-bde (Bitlocker), efsinfo (EFS)	mount –v, ls /media

Guidelines for evidence examination

วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
Journal of Criminology and Forensic Science

การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์
A Study of Guidelines in Digital Forensic Evidence Examination

จิตชนก อินถามา และ วงศ์ยศ เกิดศรี
คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

Jitchanok Inthama and Wongyos Keardsri
Faculty of Forensic Science, Royal Police Cadet Academy

Received January 25, 2021 | Revised May 19, 2021 | Accepted June 13, 2021

บทคัดย่อ

ปัจจุบันอุปกรณ์ดิจิทัลมีการใช้งานกันอย่างแพร่หลายในชีวิตประจำวันของมนุษย์ทำให้อัตราการเกิดเหตุอาชญากรรมบนระบบออนไลน์มีเพิ่มมากยิ่งขึ้น ดังนั้นขั้นตอนหรือแนวทางการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับอุปกรณ์ดิจิทัลจึงต้องมีความซับซ้อนและความน่าเชื่อถือสูงขึ้นเช่นเดียวกัน งานวิจัยเรื่องนี้จึงมีวัตถุประสงค์เพื่อศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์ของประเทศไทย โดยเป็นการศึกษาเชิงคุณภาพซึ่งแบ่งออกเป็น 2 ส่วน ส่วนแรกเป็นการศึกษาเอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานทั้งภายในและภายนอกประเทศจำนวน 4 หน่วยงาน ได้แก่ 1) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ 2) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ 3) คณะทำงานวิทยาศาสตร์เกี่ยวกับหลักฐานดิจิทัล และ 4) องค์การมาตรฐานสากล ส่วนที่สองเป็นการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลหลักในหน่วยงานทางด้านนิติวิทยาศาสตร์ของประเทศไทยจำนวน 4 หน่วยงาน ได้แก่ 1) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี 2) สถาบันนิติวิทยาศาสตร์ 3) กรมสอบสวนคดีพิเศษ และ 4) สำนักงานพิสูจน์หลักฐานตำรวจ ผลการศึกษาเอกสารสามารถสรุปขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลออกเป็น 9 ขั้นตอนและ ผลการสัมภาษณ์ผู้ให้ข้อมูลหลักทำให้เห็นถึงสภาพปัญหาในขั้นตอนการตรวจพิสูจน์หลักฐาน เช่น การไม่เข้าใจถึงวัตถุประสงค์ในการส่งตรวจพิสูจน์และการขาดองค์ความรู้และความเชี่ยวชาญของผู้ปฏิบัติงาน งานวิจัยเรื่องนี้สามารถนำไปใช้พัฒนาเป็นมาตรฐานการตรวจพิสูจน์หลักฐานทางดิจิทัลของประเทศไทยได้ในอนาคต

คำสำคัญ: ตรวจพิสูจน์หลักฐาน, หลักฐานทางดิจิทัล, แนวทาง

Abstract

Nowadays, digital devices have been widely used in the daily life of humans. Consequently, the number of cybercrimes has been increasing significantly. Moreover, the

ตารางที่ 1 สรุปขั้นตอนการตรวจพิสูจน์หลักฐานทางดิจิทัลของหน่วยงานที่เกี่ยวข้องทางนิติวิทยาศาสตร์ทั้งภายในและภายนอกประเทศที่ได้จากการวิเคราะห์เอกสารแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลของแต่ละหน่วยงาน

ขั้นตอน	หน่วยงาน			
	ETDA	NIST	SWGDE	ISO
การระบุ (Identification)	✗	✗	✗	✓
การรวบรวม (Collection)	✓	✓	✓	✓
การบรรจุและเคลื่อนย้าย (Packaging and Transportation)	✓	✗	✓	✗
การสำเนาข้อมูล (Acquisition)	✓	✓	✓	✓
การตรวจสอบ (Examination)	✗	✓	✗	✗
การวิเคราะห์ (Analysis)	✓	✓	✗	✗
การบันทึก (Document)	✓	✗	✓	✗
การรายงาน (Report)	✓	✓	✓	✗
การเก็บรักษา (Preservation)	✗	✗	✗	✓

A Study of Guidelines in Digital Forensic Evidence Examination
https://so02.tci-thaijo.org/index.php/forensic/article/download/247001/168712/

Live vs post-mortem forensics

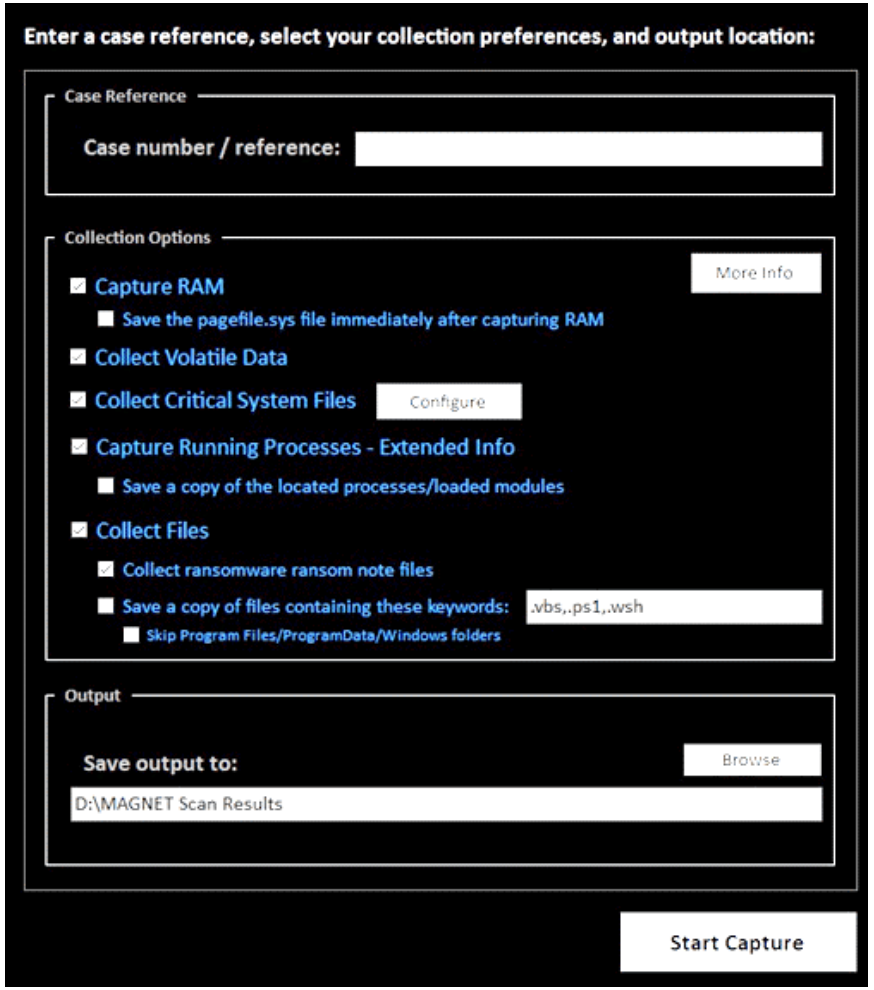
- To pull or not to pull the plug?
  - Attacker can change or destroy the evidence
  - Examiner's tools and acts may overwrite data or cause data loss
  - Can the system go back to normal operation after an unplanned switch off?
- Advantages and risks of live forensics
  - Can capture malware and encryption passwords from RAM
  - Can conduct live imaging of an encrypted drive, RAID, or non-supported file systems
  - The live system may be untrustworthy
  - Must run the forensic tool with Administrator privilege
  - Might affect the admissibility of digital evidence for cybercrime investigation

Incident Response: Live Forensics and Investigations
https://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf
Sam Bowne CNIT 121 (Summer 2023): Computer Forensics (Module 7) – Admissibility of Digital Evidence
https://samsclass.info/121/121_Sum23.shtml

Triaging and live data acquisition

Requirement ---------- Tool	independence regarding admin rights	FS artifacts and configs	external tool execution	free and open source	free download	easy extensible	multi-platform	one-shot binary (statically linked?)	collection and analysis (parsing)	active development	output format (open, easy to use)
KAPE					via form	artifact collection files are open source and separated from the binary	Windows	.NET binary + config files for artifacts			
Redline		limited set of predefined artifacts			via form		Windows			Release Date: June 8, 2018	
IRTriage						AutoIT script and re-compilation	Windows	third party tools	RegRipper output against registry hives	last commit 4 years old	
IREC					via form (or commercial version)		Windows		some parts on the filesystem, partially through HTML output		
Invoke-LiveResponse						PowerShell source code	Windows	PowerShell scripts in subfolders			
DFIR ORC						C++ and re-compilation	Windows				
CyLR						.NET code and re-compilation					
FastIR Collector						Python code and re-compilation	Windows			last commit 3 years old	
artifactcollector						Go, prepare artifacts in YAML and Go re-compilation				young project on Github, only some month old	artifactstore

Forensic Artifact Live Collection Tool Matrix
https://github.com/swisscom/ArtifactCollectionMatrix



Magnet RESPONSE
https://www.magnetforensics.com/blog/getting-started-with-magnet-response

DFIR frameworks for cloud services

Who it's for:

- All cloud customers
- Cloud service providers who need a clear framework for sharing incident response practices with customers

Cloud Incident Response Framework

Release Date: 05/04/2021

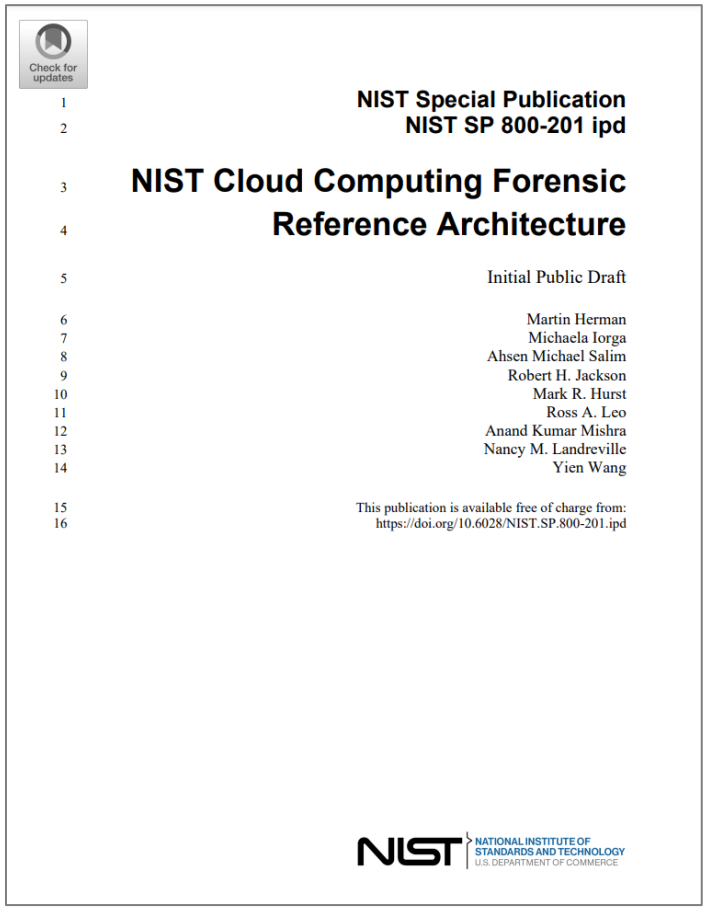
Working Group:
Cloud Incident Response

Preventive security controls cannot completely eliminate the possibility of critical data being compromised in a cyber attack. Therefore, organizations that utilize cloud services must ensure that they have a reliable cloud incident response strategy in place. Cloud incident response is simply the process used to manage cyber attacks in a cloud environment. There are several key aspects of a cloud incident response system that differentiate it from a non-cloud incident response system, notably in the areas of governance, shared responsibility, and visibility.

This framework created by the Cloud Incident Response Working Group serves as a go-to guide for cloud customers to effectively prepare for and manage cloud incidents. It explains how to assess an organization's security requirements and then opt for the appropriate level of incident protection. Cloud customers will learn how to negotiate with cloud service providers, select security capabilities that are made-to-measure, and divide security responsibilities.

Key Takeaways:

- How to effectively manage cloud incidents through the entire lifecycle of a disruptive event, including:
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-mortem
- How to coordinate and share information with stakeholders and other organizations



Check for updates

NIST Special Publication
NIST SP 800-201 ipd

NIST Cloud Computing Forensic Reference Architecture

Initial Public Draft

Martin Herman
Michaela Iorga
Ahsen Michael Salim
Robert H. Jackson
Mark R. Hurst
Ross A. Leo
Anand Kumar Mishra
Nancy M. Landreville
Yien Wang

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-201.ipd

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

CSA – Cloud Incident Response Framework
https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/

NIST Cloud Computing Forensic Reference Architecture
https://csrc.nist.gov/pubs/sp/800/201/ipd

DFIR frameworks for OT systems

DIGITAL	Device Time/Date	Time and date found on the system.
	Last-known Approved Configuration	Last known approved configuration, factory acceptance test (FAT) and site acceptance test (SAT) approved configurations,
	OS Version	OS version documented and found running at the time of collection.
	Firmware	Firmware running on the device at the time of collection and firmware documented in last update or FAT/SAT.
	CPU/Memory Usage	Percentage of CPU/memory available and percentage used.
	Running Processes	Individual processes running on the device.
	Logs and Diagnostic Data	Related security logs and diagnostic data available for the device.
	Network Traffic	Network traffic to and from the device.
	Memory Dump	If feasible.
PHYSICAL	Device Information	Device equipment identifier, manufacturer, model, serial number, and any other unique identifiers.
	Function	Description of the function of the device (e.g. PLC controlling temperature of a specific valve).
	Location	Physical location of the device (e.g. site, building, room, panel, etc.) and physical access logs, if applicable.
	Connections and Protocols	Physical connections for the device, wiring diagrams, MAC address, and documented protocols used.
	Photos	Status of LEDs, tamper tape seals, port blockers, wiring, devices found connected at the time of collection, and other physical
	Temperature	Temperature of the device (may indicate high CPU usage). This can be collected using an infrared temperature gun.

MANDIANT

Mandiant Digital Forensics and Incident Response Framework for Embedded OT Systems
https://www.mandiant.com/resources/blog/mandiant-dfir-framework-ot

NIST Search NIST Menu

PUBLICATIONS

Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)

Published: June 22, 2022

Author(s)
Eran Salfati, Michael Pease

Abstract
This document provides a new Incident Handling framework dedicated to Operational Technology. This framework expands the traditional technical steps by giving an Incident Response procedure based on the event escalation and provides techniques for OT Digital Forensics. It includes an overview with general terms explanation and a list of unique properties of OT DFIR, the preparation that should be done to establish an OT Incident Response Team, and finally, the suggested OT Incident Handling framework in detail.

Citation: NIST Interagency/Internal Report (NISTIR) - 8428

Report Number: 8428

NIST Pub Series: NIST Interagency/Internal Report (NISTIR)

Pub Type: NIST Pubs

NISTIR 8428 – Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)
https://www.nist.gov/publications/digital-forensics-and-incident-response-dfir-framework-operational-technology-ot

Evidence interpretation

- Data recovery
  - Recover deleted file/record
  - File carving
- Parsing and navigation
  - File system
  - Data stream
- Identification and extraction of artifacts
  - Keyword search
  - Data extraction
  - Decryption
- Analysis of results
  - Timeline analysis

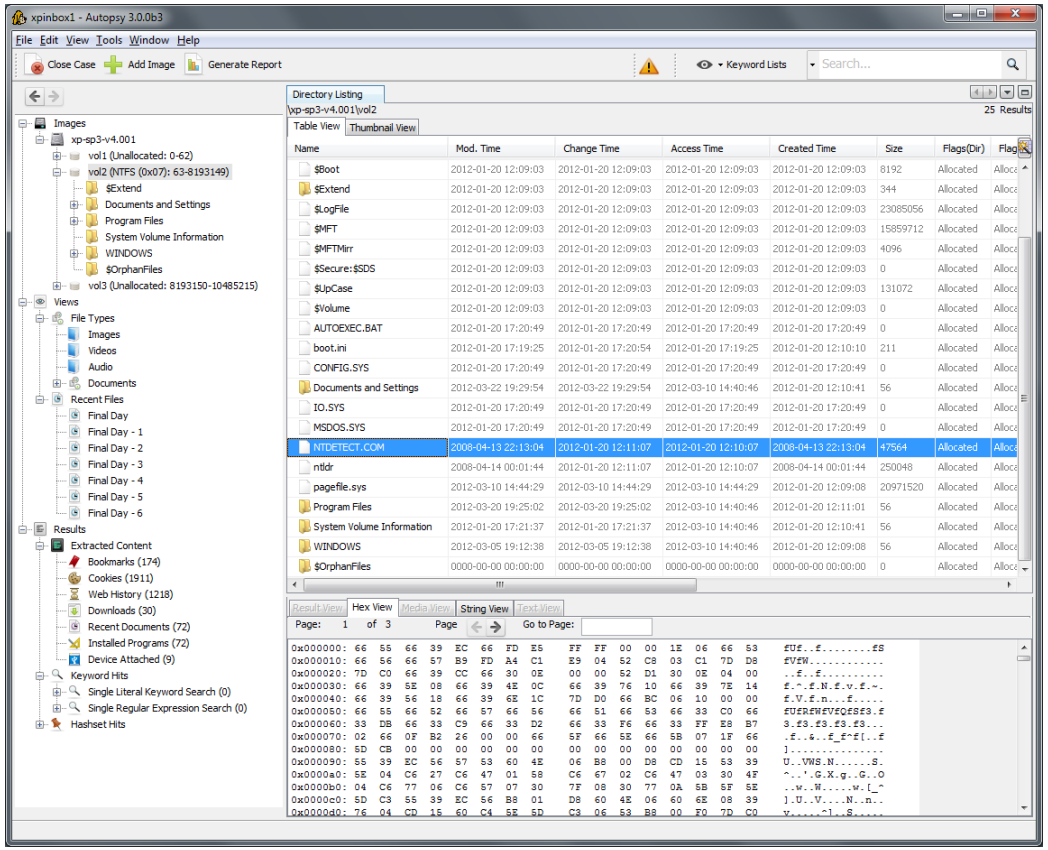


Photo: https://www.sleuthkit.org/autopsy/

Digital forensics report

MFEC Public Company Limited

Digital forensics report

Table of Contents

MFEC Public Company Limited

Digital forensics report

Executive Summary

เมื่อวันที่ [redacted] ทีม MFEC CSOC ได้รับการประสานเพื่อตรวจวิเคราะห์เว็บไซต์ [redacted] เพื่อระบุสาเหตุของการโจมตี พร้อมเสนอแนวทางการป้องกันและแก้ไขปัญหา

ผลการวิเคราะห์ พบว่าเว็บไซต์ [redacted] ถูกโจมตีโดยใช้เครื่องมือ anonymousfox ซึ่งเป็นเครื่องมือสำเร็จรูปที่มีความสามารถในการโจมตีเว็บไซต์ที่ใช้งาน WordPress พร้อมทั้งสามารถยึดระบบบริหารจัดการเว็บไซต์ เช่น cPanel หรือ WebHost Manager นอกจากนี้ ยังพบข้อมูลว่าเว็บไซต์ดังกล่าวถูกโจมตีสำเร็จตั้งแต่ [redacted] หรือก่อนหน้านั้น รวมทั้งถูกฝัง backdoor เพื่อใช้เข้าถึงระบบในภายหลังไว้เป็นจำนวนมาก

แนวทางการป้องกันและแก้ไขปัญหา [redacted]

TYPES OF DIGITAL FORENSICS REPORTS

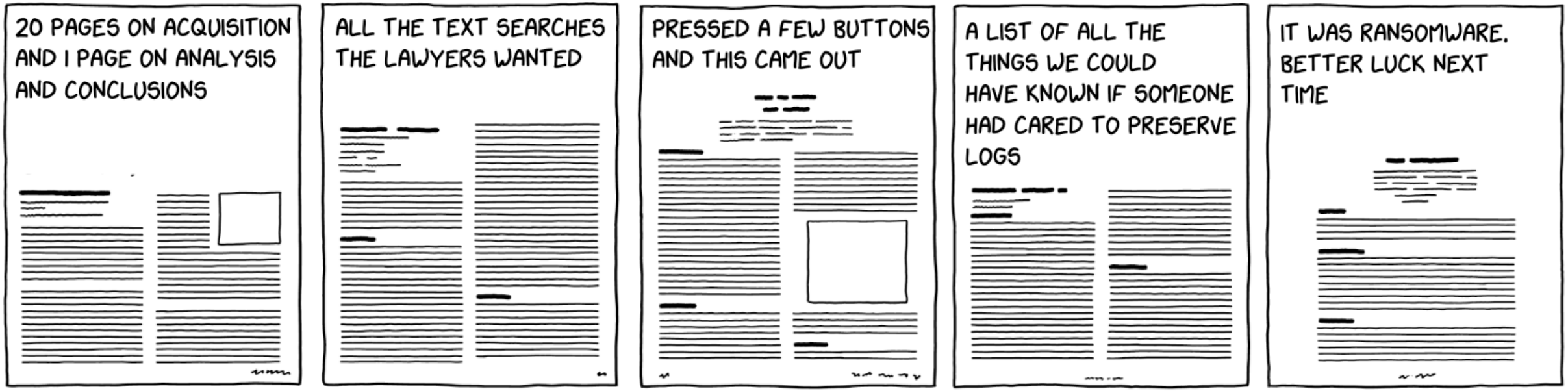
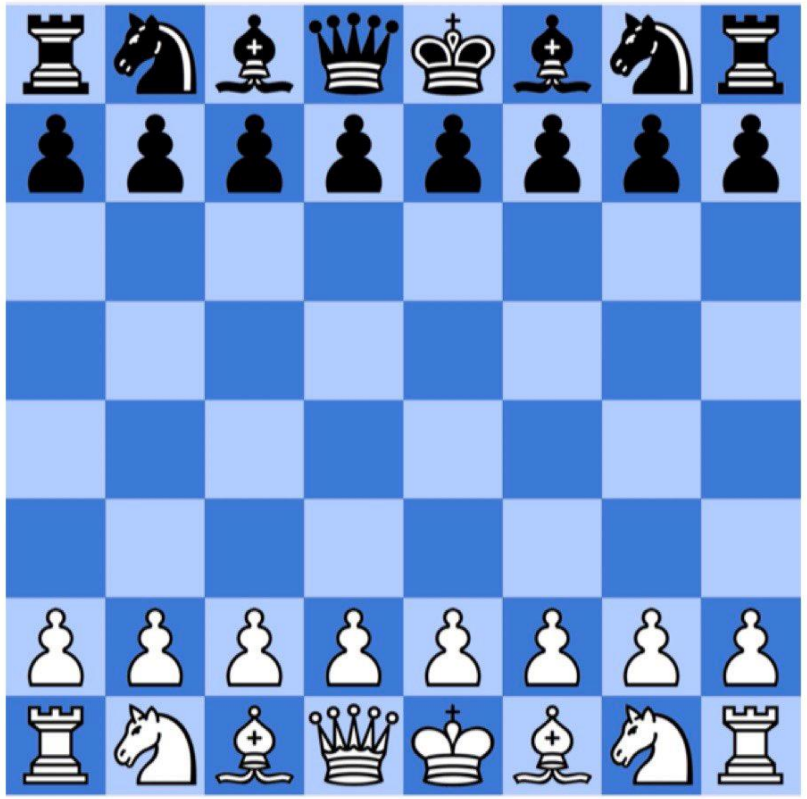


Photo: https://twitter.com/AlexisBrignoni/status/1390539300748603392

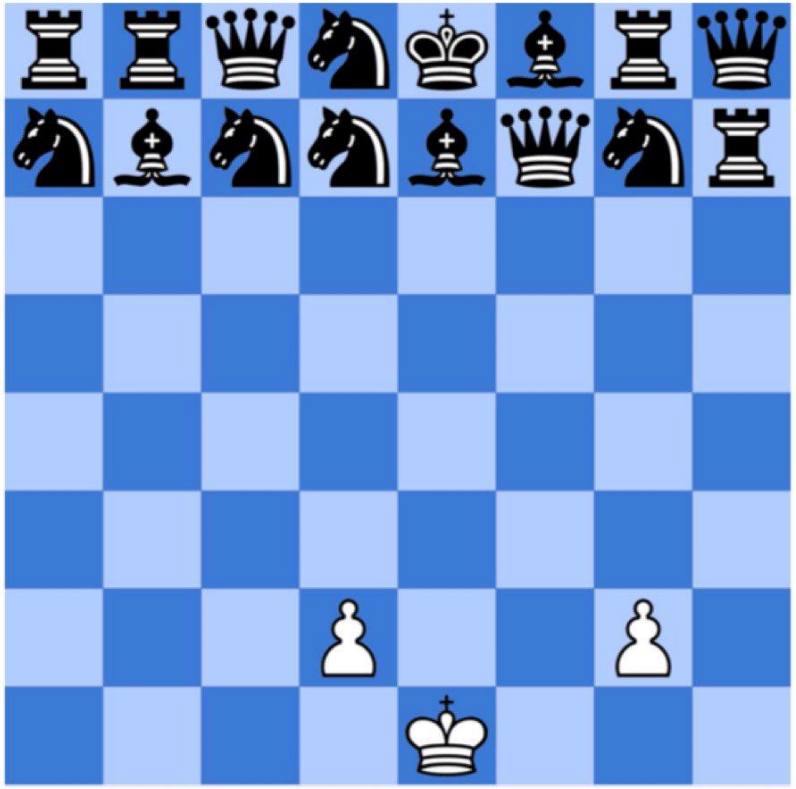
Limitations and concerns

- Dependent on an understanding of how the computer activities, tools, and techniques work
- Every digital forensic technique should undergo peer review, formal testing, or error rate analysis.
  - It is not feasible to test all combinations of tools, run time environments, and digital evidence sources.
- Standard operating procedure and legal
  - Will pieces of evidence and processes accept in the court?

Asymmetry between attackers and defenders



Theory



Real world

Photo: https://twitter.com/z3r0trust/status/1394765371303862276

Computer Forensics Tool Testing (CFTT)

NIST

Search NIST

Menu

Information Technology Laboratory / Software and Systems Division

SOFTWARE QUALITY GROUP

Computer Forensics Tool Testing Program (CFTT)

- CFTT General Information +
- CFTT Technical Information +
- Federated Testing Project
- CFReDS
- Computer Forensics Tool Catalog
- Software & Algorithms Catalog
- Digital Evidence Preservation: Considerations for Evidence Handlers
- Useful Links

Computer Forensics Tool Testing Program (CFTT)

Welcome to the Computer Forensics Tool Testing (CFTT) Project Web Site.

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. A capability is required to ensure that forensic software tools consistently produce accurate and objective test results. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing.

The Computer Forensics Tool Testing Program is a project in The Software and Systems Division supported by the Special Programs Office and the Department of Homeland Security. Through the Cyber Security Division Cyber Forensics project, the Department of Homeland Security's Science and Technology partners with the NIST CFTT project to provide forensic tool testing reports to the public.

NEW: Federated Testing -- Guidance for common test methods & test report sharing via downloaded CD iso is available.

Computer Forensic Tool Testing (CFTT) Reports

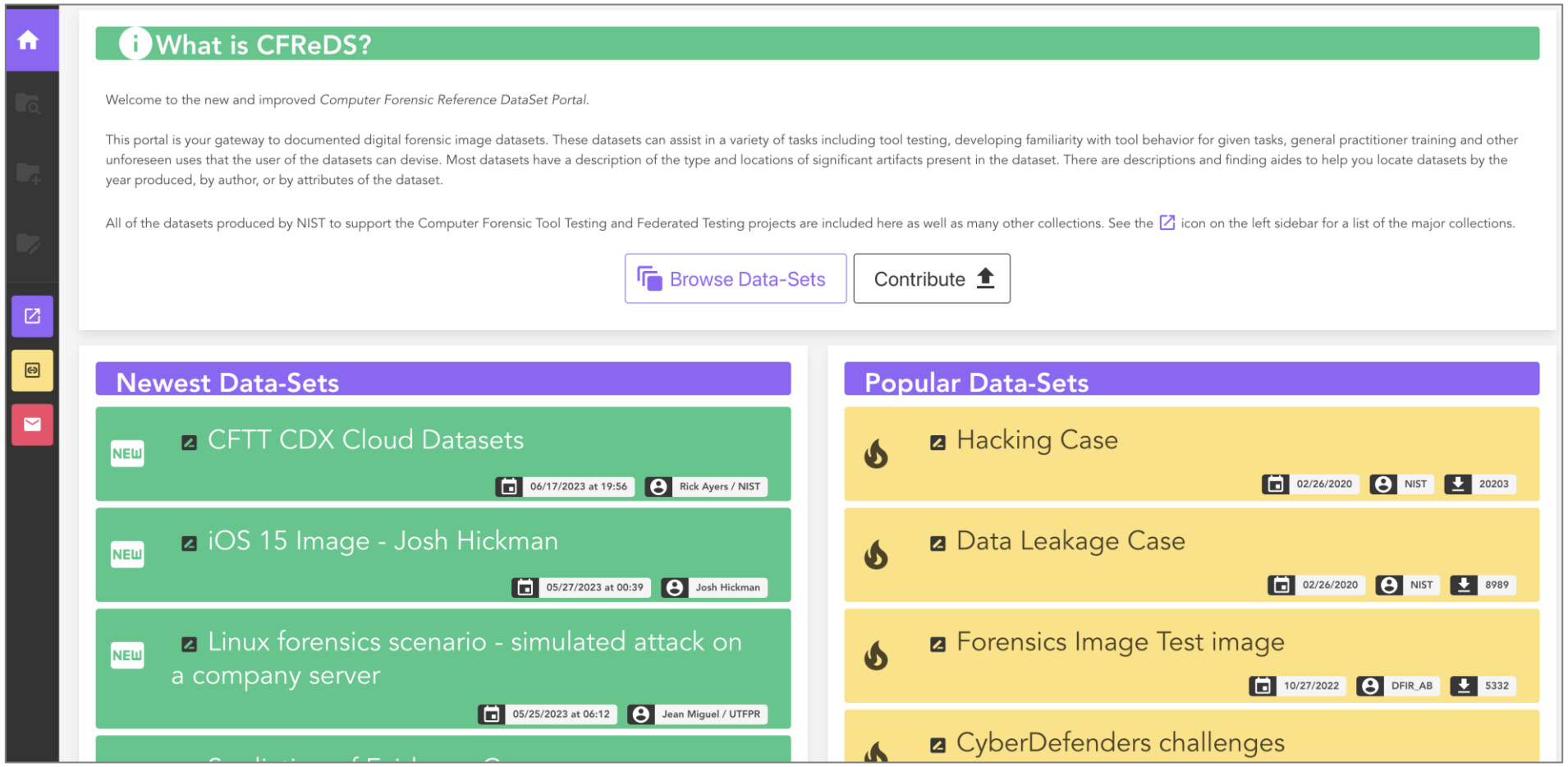
S&T partners with the NIST Computer Forensic Tool Testing (CFTT) program to provide forensic tool testing reports to the public. The CFTT project has established a methodology for testing computer forensic software tools utilizing tool specifications, test procedures, test criteria, test sets, and test hardware. Report results encourage developers to update and improve tools and provide end users with information on tool capabilities necessary for use and acquisition.

Reports, organized by tool category, can be accessed and downloaded via the links below. Reports within each category are organized by publication date (newest to oldest).

- Binary Image (JTAG, Chip-Off) Decoding and Analysis Tools
- Deleted File Recovery and Active File Listing
- Digital Data Acquisition
- Disk Imaging
- Forensic Media Preparation
- Graphic File Carving
- Hardware Write Block
- Mobile Device Acquisition
- Software Write Block
- SQLite Data Recovery Tools
- String Search Tool
- Video File Carving
- Write Protected Drive
- Windows Registry Forensic Tool

https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Computer Forensic Reference DataSet (CFReDS)



https://cfreds.nist.gov/

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

NIST SP 800-86

Guide to Integrating Forensic Techniques into Incident Response

Date Published: August 2006

Author(s)

Karen Kent (NIST), Suzanne Chevalier (BAH), Tim Grance (NIST), Hung Dang (BAH)

Abstract

This publication is intended to help organizations in investigating computer security incidents and troubleshooting some information technology (IT) operational problems by providing practical guidance on performing computer and network forensics. The guide presents forensics from an IT view, not a law enforcement view. Specifically, the publication describes the processes for performing effective forensics activities and provides advice regarding different data sources, including files, operating systems (OS), network traffic, and applications. The publication is not to be used as an all-inclusive step-by-step guide for executing a digital forensic investigation or construed as legal advice. Its purpose is to inform readers of various technologies and potential ways of using them in performing incident response or troubleshooting activities. Readers are advised to apply the recommended practices only after consulting with management and legal counsel for compliance concerning laws and regulations (i.e., local, state, Federal, and international) that pertain to their situation.

Keywords

FISMA; Forensics; Incident Response

Control Families

Audit and Accountability; Configuration Management; Contingency Planning; Identification and Authentication; Media Protection; Physical and Environmental Protection; System and Information Integrity

DOCUMENTATION

Publication:

https://doi.org/10.6028/NIST.SP.800-86

Download URL

Supplemental Material:

None available

Document History:

09/01/06: SP 800-86 (Final)

TOPICS

Security and Privacy

incident response

Applications

forensics

Laws and Regulations

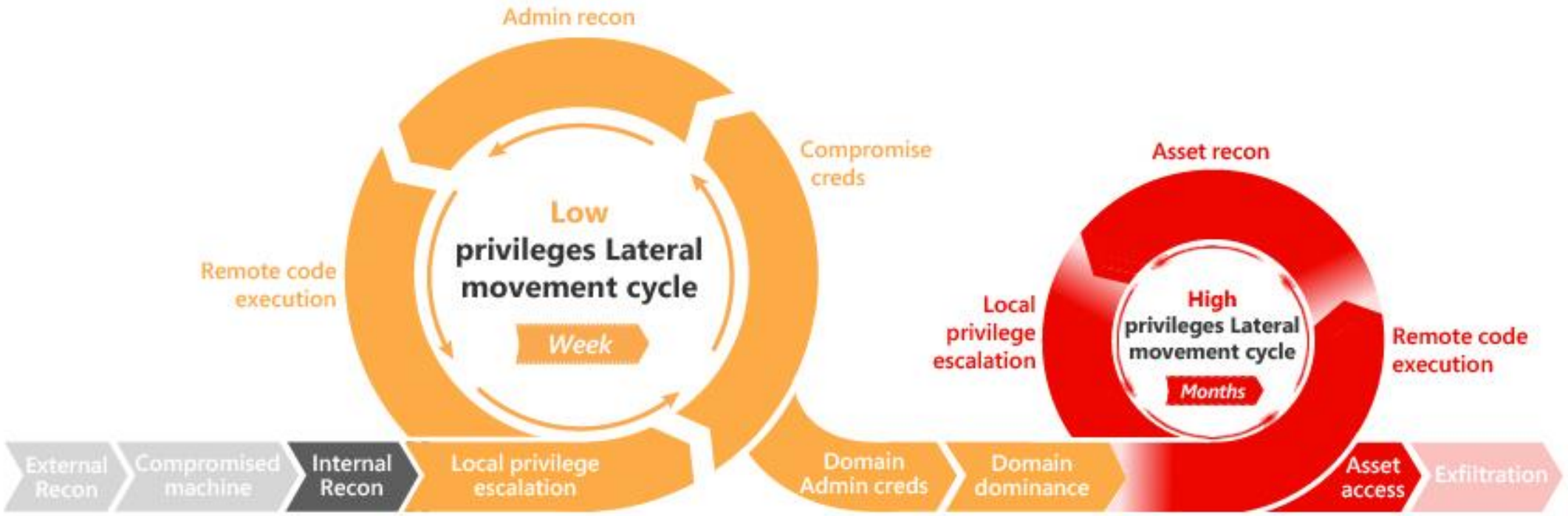
Federal Information Security Modernization Act

https://csrc.nist.gov/pubs/sp/800/86/final

Evidence examination & analysis

- Using data from data files
  - File system, MAC times, data integrity
- Using data from operating systems
  - Volatile/Non-volatile data
  - OS data
- Using data from network traffic
  - Identifying network data sources
  - collecting and examining network activities
- Using data from applications
  - Email, web, file sharing, security applications

Attack kill chain



Microsoft – Advanced Threat Analytics
https://learn.microsoft.com/en-us/advanced-threat-analytics/ata-threats

Adversary tactics, techniques, and data sources

Tactic	Common Techniques	Log and Event Sources	Indicators
Initial Access	Phishing [T1566], Drive-by Compromise [T1189], Exploit Public Facing Application [T1190], External Remote Services [T1133]	Email, web proxy, server application logs, IDS/IPS	Phishing, redirect, and payload servers (domains and IP addresses), delivery mechanisms (lures, macros, downloaders, droppers, etc.), compromised credentials, web shells
Execution	Command and Script Interpreters [T1059], Exploitation for Client Execution [T1203]	Host event logs, Windows event logs, Sysmon, anti-malware, EDR, PowerShell logs	Invocation of command or scripting interpreter, exploitation, API calls, tools, malware, payloads
Persistence	Account Manipulation [T1098], Scheduled Task/Job [T1053], Valid Accounts [T1078]	Host event logs, Authentication logs, Registry	Scheduled Tasks, registry keys, autoruns, etc.
Lateral Movement	Exploitation of Remote Services [T1210], Remote Session Hijacking [T1563], Software Deployment Tools [T1072]	Internal network logs, host event logs, Application Logs	Mismatch of users and applications/credentials, workstation to workstation communication, beaconing from hosts not intended to be internet accessible, etc.
Credential Access	Brute Force [T1110], Modify Authentication Process [T1556], Man-in-the-Middle [T1557]	Authentication Logs, Domain Controller Logs, network traffic monitoring	LSASS reads, command or scripting interpreters accessing LSASS, etc.
C2	Application Layer Protocol [T1071], Protocol Tunneling [T1572]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	C2 domains, IP addresses
Exfiltration	Exfiltration Over C2 Channel [T1041], Exfiltration Over Alternative Protocol [T1048]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	Domains, URLs, IP addresses, IDS/IPS signatures

CISA - Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Competency requirements for investigator

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่
พ.ศ. ๒๕๖๔

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ด้านการบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) แล้วแต่กรณี ดังต่อไปนี้

ด้านที่ห้า การพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Computer Forensics and Forensic Readiness
๒	Computer Forensics Investigation Process - Obtain Search Warrant - Evaluate and Secure the Scene - Collect the Evidence - Secure the Evidence and Chain of Custody - Acquire Data and Analyze Data - Assess Evidence and Case - Testify as Expert Witness
๓	Defeating Anti-Forensics Techniques
๔	Operating System Forensics
๕	Network Forensics
๖	Web Attack Forensics
๗	Database Forensics
๘	Cloud Forensics
๙	Wireless Forensics
๑๐	Malware Forensics
๑๑	Email-Crime Forensics
๑๒	Mobile Forensics
๑๓	Application Password Cracker
๑๔	Investigative Reports

NCSC Announcement https://drive.ncsa.or.th/s/rB7CGDmmc55yJQ6

Lead The Digital Forensics Movement By Becoming A **Computer Hacking Forensic Investigator** with **EC-Council**

Become a C|HFI

Program Information

What's New in CHFI | Course Outline | Who is it for? | About the Exam | Job Roles | Brochure

Course Outline

Module 01: Computer Forensics in Today's World	**Module 09:** Investigating Web Attacks
Module 02: Computer Forensics Investigation Process	**Module 10:** Dark Web Forensics
Module 03: Understanding Hard Disks and File Systems	**Module 11:** Database Forensics
Module 04: Data Acquisition and Duplication	**Module 12:** Cloud Forensics
Module 05: Defeating Anti-Forensics Techniques	**Module 13:** Investigating Email Crimes
Module 06: Windows Forensics	**Module 14:** Malware Forensics
Module 07: Linux and Mac Forensics	**Module 15:** Mobile Forensics
Module 08: Network Forensics	**Module 16:** IoT Forensics

EC-Council CHFI
https://www.eccouncil.org/train-certify/computer-hacking-forensic-investigator-chfi/

APPENDIX A: DFL SKILLSET CHECKLIST

The following is a recommendation of skillsets for the DFL Examiner. The reader shall take note that the list is non-exhaustive and needs to be updated from time to time.

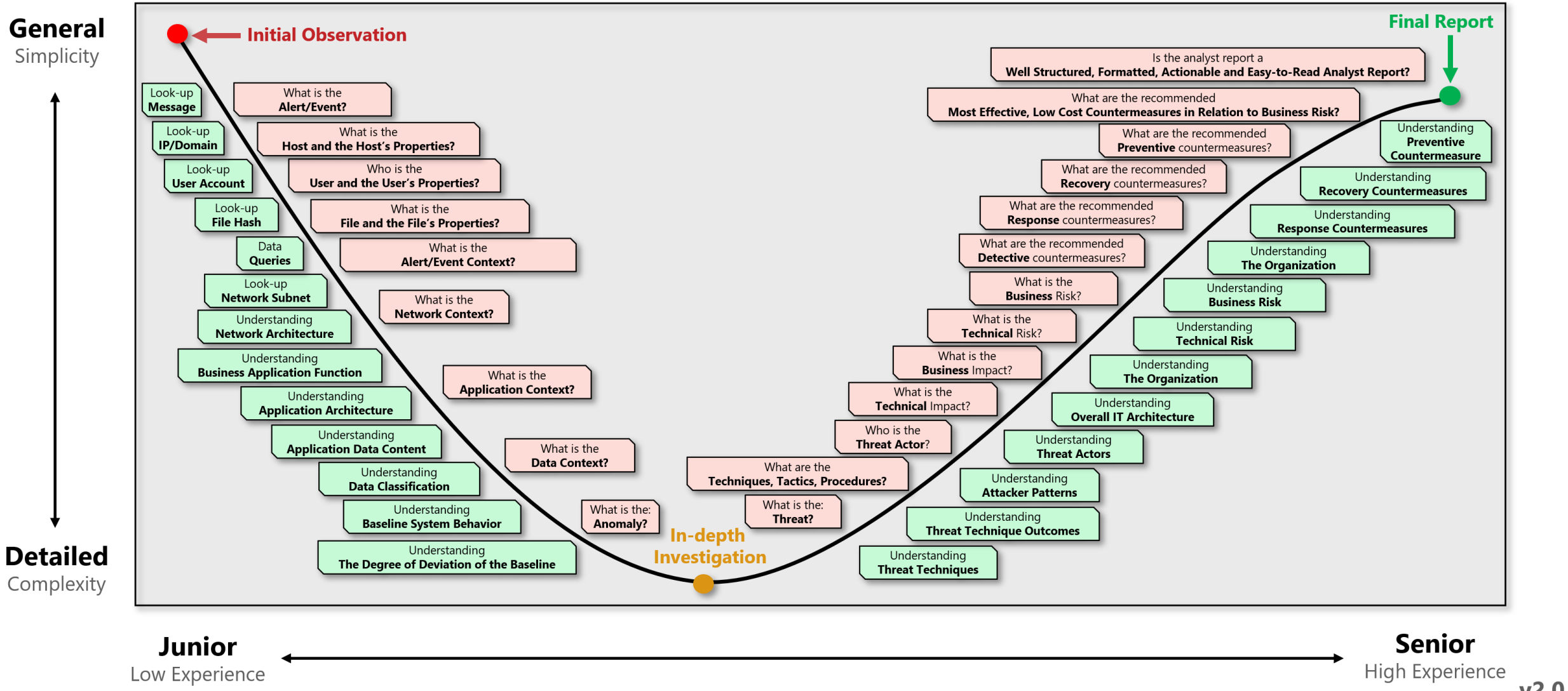
Category	Topic	Skillset	
Foundation	Computer Foundation	Organization of computer; How computer stores data; Bits & bytes; Evolution of digital media and storage system.	☐
	File System	Decimal, hexadecimal, binary; Little endian, big endian; Sectors, cluster, slack space; Metadata, data, filename; FAT, NTFS, EXT, HFS.	☐
	Introduction to Investigation and Digital Forensics	Law enforcement and regulators; Introduction to forensic science, electronic evidence and its nature; Categories of electronic evidence; Methodology; Forensics terminologies.	☐
Identification	Information Gathering	Gather facts of the case online; Preserve the gathered facts.	☐
Collection and Examination	Collection and Examination	First responder roles and SOP; Dead acquisition and live acquisition; Choosing the best data acquisition method; Triage method; Triage tool.	☐
Analysis	Data Recovery	Storage technology; Damaged hard disk and flash drive symptoms; Logical and physical recovery; Data recovery tools; Recovery of data using tools.	☐
	Computer Forensics	Operating systems technology; Metadata, registry, artefact; Data Extraction; Data analysis; Data hiding technique; Analytics for large sets of data; Memory Analysis.	☐
	Mobile Phone Forensics	Mobile phone Technology and evolution, User, telecommunication provider technology, types of data, acquire and analysis tools, preservation of data.	☐
	Network Forensics	Network Types; Internet history files and Cookies; User Credentials; Network forensic tools; Reading packets.	☐
	Audio, Video and Image Forensics	Understanding the technology; Enhancement; File Authentication; Comparison.	☐
	Emerging Technology:	Understanding the technology; Accessing data from the device; Data Extraction; Data	☐

	- Social Media Forensic - Database Forensic - Drone Forensic - Vehicle Forensic - Shipbourne forensic - Cryptocurrency Forensic - Biometric Forensic	analysis; Data interpretation; Reporting the findings.	☐
Presentation	Report Writing	The format of the report; Effective result presentation to stakeholders.	☐
	Law & Mock Court	Laws related to cases; International Law; International Collaboration; Presenting expert testimony in court; Introduction to Court structure; Submitting electronic evidence in court.	☐
Etiquette	Etiquette	Professional Code of ethics, ethical & non-ethical code of conduct.	☐
Lab Management	Quality Management	Understanding standards; Conducting Audit; Quality Management System.	☐
	Health & Safety	Identify hazards; Health and Safety measures; Self-protection.	☐

INTERPOL – Global guidelines for digital forensics laboratories
https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics

Cyber Security Analyst Maturity Curve

*"A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**"*



v2.0

http://correlatedsecurity.com/cyber-security-analyst-maturity-curve/

Cooperation between CSIRT and LE

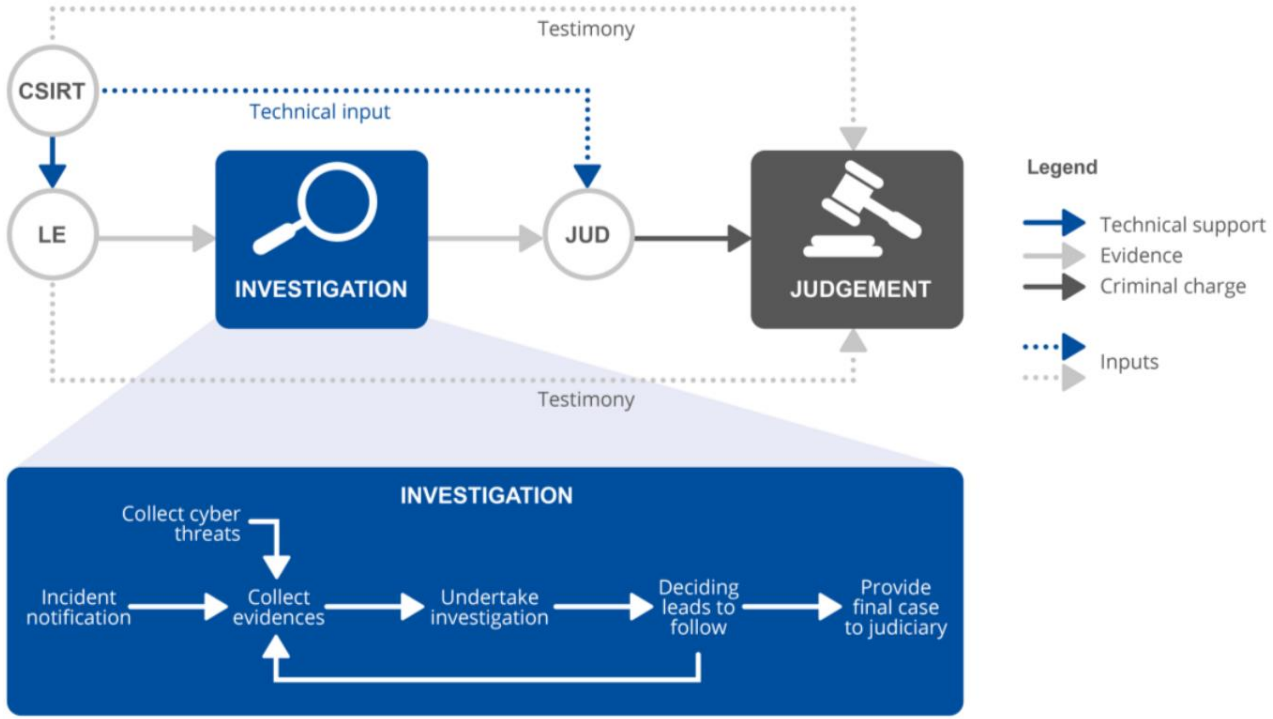


Table 2: ISO/IEC standards for the cybercrime investigation phase

ISO/IEC standard	Title
ISO/IEC 27050-2:2018	Information technology – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery
ISO/IEC 27050-3:2017	Information technology – Security techniques – Electronic discovery – Part 3: Code of practice for electronic discovery
ISO: 27050-1:2016	Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts
ISO/IEC 30121:2015	Information technology – Governance of digital forensic risk framework
ISO/IEC 27043:2015	Information technology – Security techniques – Incident investigation principles and processes
ISO/IEC 27042:2015	Information technology – Security techniques – Guidelines for the analysis and Interpretation of digital evidence
ISO/IEC 27041:2015	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 17020:2012	Conformity assessment – Requirements for the operation of various types of bodies performing inspection

ENISA - Roadmap on the cooperation between CSIRT and LE
https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

CSIRT and LE: Cooperation problems

Not all cyber incidents are cybercrimes (so LE do not need to be informed) and not all cybercrimes are considered cyber incidents (so CSIRTs do not need to be informed). This means that LE and CSIRTs do not always have the same interest in incidents or investigations, which also affects the way they further handle each case. Since cybercrime crosses borders, cooperation among countries is often crucial in the fight against it. In this regard, at least three difficulties are identified:

3. **Difficulties related to different mindset approaches**. CSIRT, LE and the judiciary have different approaches or mindsets, which also derives from the different educational and scientific backgrounds. In particular, CSIRTs have a 'technical mentality' while the judiciary has a 'legal mentality'. The LE have partly a 'legal mentality' and partly a 'technical mentality' that is entrenched in how society operates in the area of crime. The different mentalities make communication among these three entities not always easy. This can also lead to limitations of cooperation or at least a slowdown in cooperation.

ENISA - Roadmap on the cooperation between CSIRT and LE
https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

Traditional vs Enterprise forensics

Traditional forensics	Enterprise forensics
Scope • Small amount of machines/devices Process • Memory acquisition • Storage/Disk acquisition • Network artifacts collection Concerns • Business continuity • Time consumption	Scope • Large scale DFIR • Varies environment (remote, cloud, VM, etc.) Process • Isolation, snapshot, triage, etc. • Remote/live forensics Concerns • Evidence preservation • Legal and court testimony

Forensic Focus - Enterprise Forensics: Traditions vs Reality in Modern DFIR
https://www.forensicfocus.com/webinars/enterprise-forensics-traditions-vs-reality-in-modern-dfir/

Anti-forensics

Purposes

- Making investigation more complicated and time-consuming
- Making evidences difficult or impossible to obtain

Methods

- Artifact wiping
- Data hiding
- Trail obfuscation
- Encryption
- Steganography
- Attack against forensic tool and methods
- Self-destruction/kill-switch

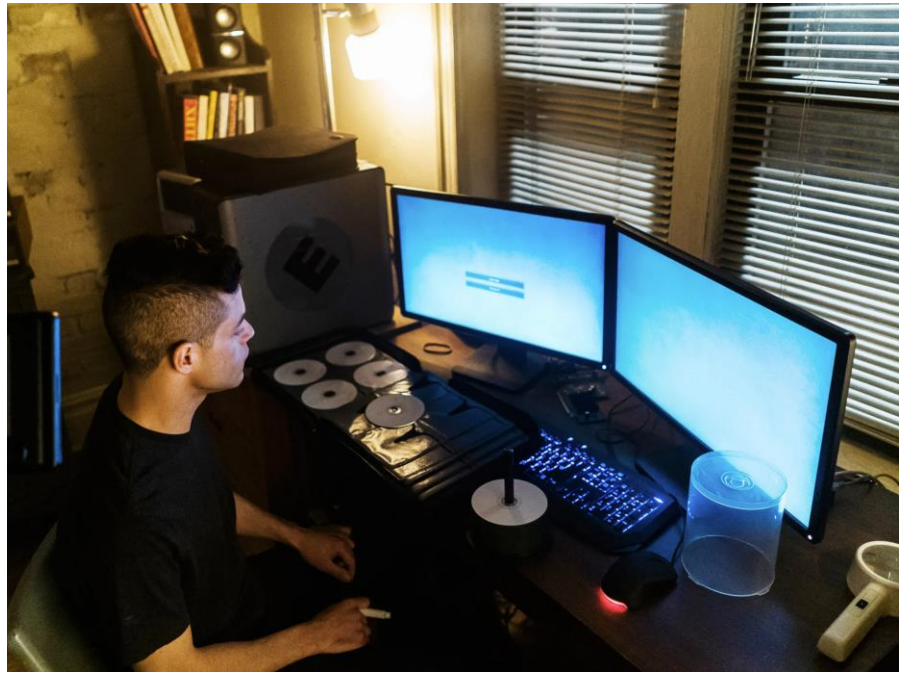
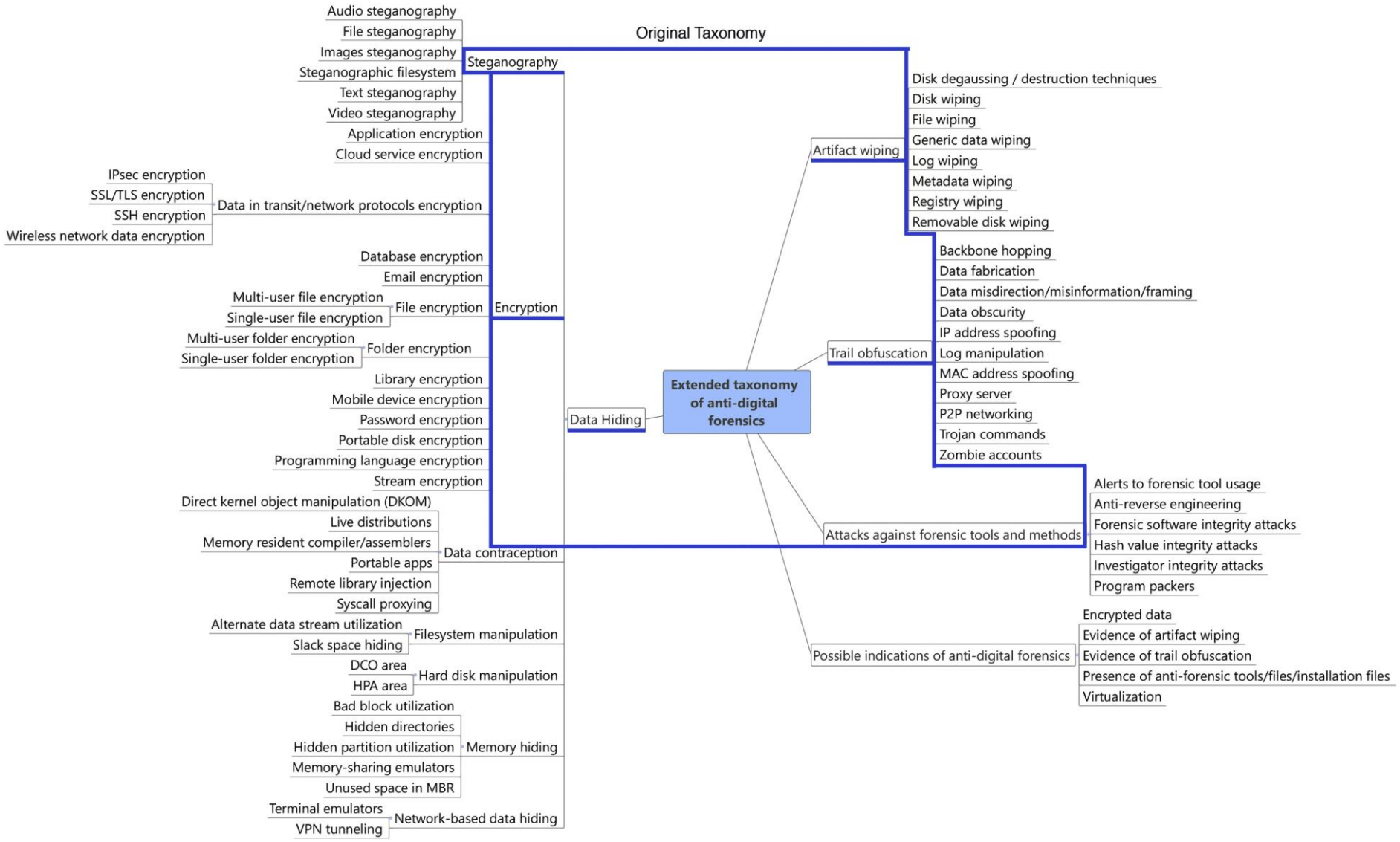


Photo: https://www.wired.com/2016/07/mr-robot-hack-check-s2e2/

Awesome anti-forensics
https://github.com/shadawck/awesome-anti-forensic

* Items underlined and inside the blue frame were categories previously identified in the original anti-forensics taxonomy proposed by Rogers (2006). Our taxonomy is an extended, more granular version of the old one.



Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy
https://www.sciencedirect.com/science/article/pii/S1742287616300378

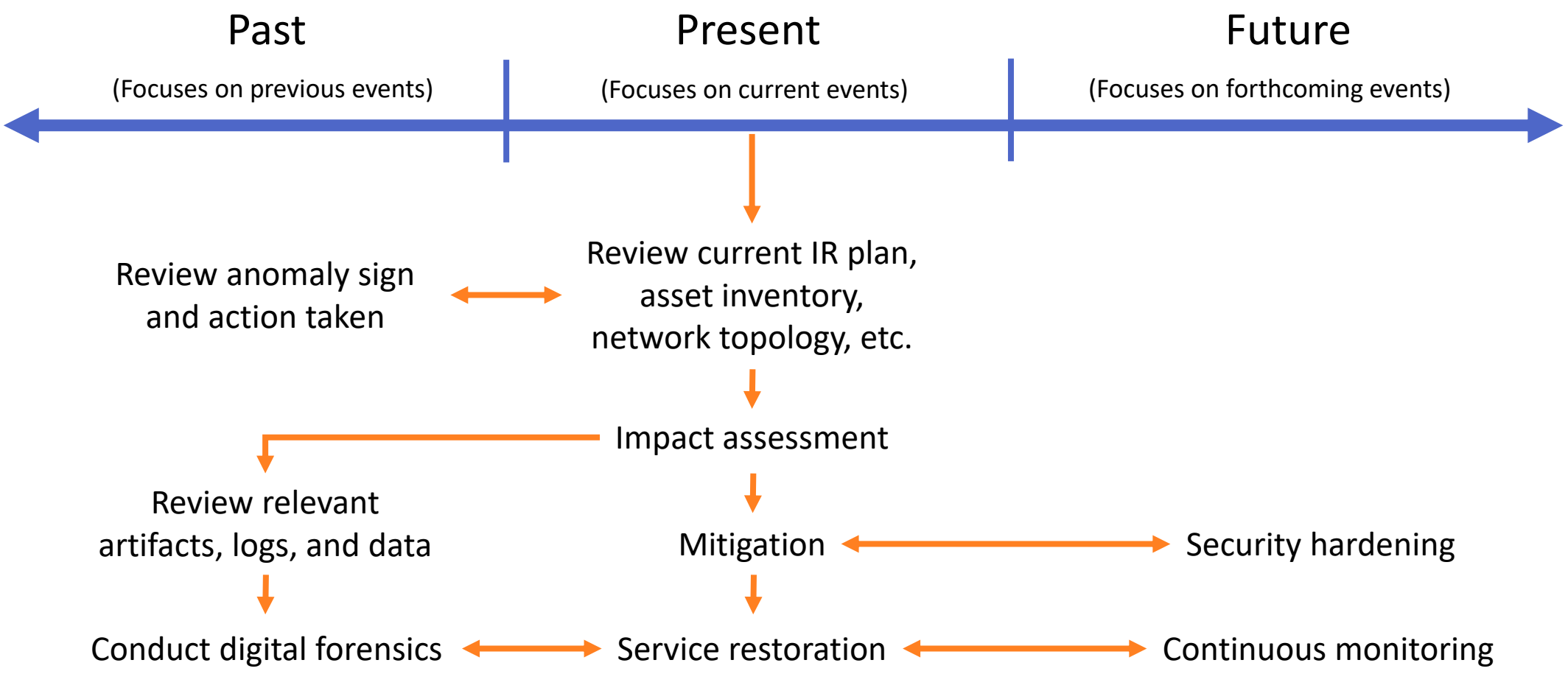
Case Studies

Case #1: Live incident response

Scenarios

- A large organization has been informed by a security researcher that their email server have been compromised
- Admin reviewed network log and found suspicious activities that indicate backdoor and data exfiltration
- The organization will conduct the most important event in the next few days

(Simplified) DFIR activities



Artifact and information collection – host

Host-Based Artifacts

- Running Processes
- Running Services
- Parent-Child Process Trees
- Integrity Hash of Background Executables
- Installed Applications
- Local and Domain Users
- Unusual Authentications
- Non-Standard Formatted Usernames
- Listening Ports and Associated Services
- Domain Name System (DNS) Resolution Settings and Static Routes
- Established and Recent Network Connections
- Run Key and other AutoRun Persistence
- Scheduled Tasks
- Artifacts of Execution (Prefetch and Shimcache)
- Event logs
- Anti-virus detections

Information to Review for Host Analysis

- Identify any process that is not signed and is connecting to the internet looking for beaconing or significant data transfers.
- Collect all PowerShell command line requests looking for Base64-encoded commands to help identify malicious fileless attacks.
- Look for excessive `.RAR`, `7zip`, or `WinZip` processes, especially with suspicious file names, to help discover exfiltration staging (suspicious file names include naming conventions such as, `1.zip`, `2.zip`, etc.).
- Collect all user logins and look for outlier behavior, such as a time of login that is out of the ordinary for the user or a login from an Internet Protocol (IP) address not normally used by the user.
- On Linux/Unix operating systems (OSs) and services, collect all `cron` and `systemd /etc/passwd` files looking for unusual accounts and log files, such as accounts that appear to be `system / proc` users but have an interactive shell such as `/bin/bash` rather than `/bin/false/nologin`
- On Microsoft OSs, collect Scheduled Tasks, Group Policy Objects (GPO), and Windows Management Instrumentation (WMI) database storage on hosts of interest looking for malicious persistence.
- Use the Microsoft Windows Sysinternals Autoruns tool, which allows IT security practitioners to view—and, if needed, easily disable—most programs that automatically load onto the system.
- Check the Windows registry and Volume Shadow Copy Service for evidence of intrusion.
- Consider blocking script files like `.js`, `.vbs`, `.zip`, `.7z`, `.sfx` and even Microsoft Office documents or PDFs.
- Collect any scripts or binary ELF files from `/dev/shm/tmp` and `/var/tmp`.
- Kernel modules listed (lsmod) for signs of a rootkit; dmesg command output can show signs of rootkit loading and device attachment amongst other things.
- Archive contents of `/var/log` for all hosts.
- Archive output from journald. These logs are pretty much the same as /var/log; however, they provide some integrity checking and are not as easy to modify. This will eventually replace the /var/log contents for some aspects of the system. Check for additional Secure Shell (SSH) keys added to user's `authorized_keys`.

CISA - Technical Approaches to Uncovering and Remediating Malicious Activity
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a

Artifact and information collection – network

Network-Based Artifacts

- Anomalous DNS traffic and activity, unexpected DNS resolution servers, unauthorized DNS zone transfers, data exfiltration through DNS, and changes to host files
- Remote Desktop Protocol (RDP), virtual private network (VPN) sessions, SSH terminal connections, and other remote abilities to evaluate for inbound connections, unapproved third-party tools, cleartext information, and unauthorized lateral movement
- Uniform Resource Identifier (URI) strings, user agent strings, and proxy enforcement actions for abusive, suspicious, or malicious website access
- Hypertext Transfer Protocol Secure/Secure Sockets Layer (HTTPS/SSL)
- Unauthorized connections to known threat indicators
- Telnet
- Internet Relay Chat (IRC)
- File Transfer Protocol (FTP)

Information to Review for Network Analysis

- Look for new connections on previously unused ports.
- Look for traffic patterns related to time, frequency, and byte count of the connections.
- Preserve proxy logs. Add in the URI parameters to the event log if possible.
- Disable LLMNR on the corporate network; if unable to disable, collect LLMNR (UDP port 5355) and NetBIOS-NS (UDP port 137).
- Review changes to routing tables, such as weighting, static entries, gateways, and peer relationships.

CISA - Technical Approaches to Uncovering and Remediating Malicious Activity
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a

Common mistakes in incident handling

- **Mitigating the affected systems before responders can protect and recover data**
  - This can cause the loss of volatile data such as memory and other host-based artifacts.
  - The adversary may notice and change their tactics, techniques, and procedures.
- **Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)**
  - These actions can tip off the adversary that they have been detected.
- **Preemptively blocking adversary infrastructure**
  - Network infrastructure is fairly inexpensive. An adversary can easily change to new command and control infrastructure, and you will lose visibility of their activity.
- **Preemptive credential resets**
  - Adversary likely has multiple credentials, or worse, has access to your entire Active Directory.
  - Adversary will use other credentials, create new credentials, or forge tickets.
- **Failure to preserve or collect log data that could be critical to identifying access to the compromised systems**
  - If critical log types are not collected, or are not retained for a sufficient length of time, key information about the incident may not be determinable. Retain log data for at least one year.
- **Communicating over the same network as the incident response is being conducted (ensure all communications are held out-of-band)**
- **Only fixing the symptoms, not the root cause**
  - Playing "whack-a-mole" by blocking an IP address—without taking steps to determine what the binary is and how it got there—leaves the adversary an opportunity to change tactics and retain access to the network.

COMMON MISSTEPS

Common missteps an organization can make when first responding

CISA - Technical Approaches to Uncovering and Remediating Malicious Activity
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a

Limitations and concerns

[REDACTED]

Virtual machine data acquisition

Data Collection

Suspend the Virtual Machine before taking memory images.

Virtual Box

Memory

- Identify the VM's UUID:
vboxmanage list vms
- Create a snapshot of the VM's memory:
vboxmanage debugvm <VM_UUID> dumpvm-core --filename win10-mem.raw

Disk

- Identify the VM's UUID:
vboxmanage list vms
- Identify the VM's disk UUID:
vboxmanage showvminfo <VM_UUID>
Note the UUID of the disk in row IDE Controller
- Export the disk using the disk UUID:
vboxmanage clonemedium disk <disk_UUID>

VMWare

Memory

- Collect the .vmem and associated .vmss and .vmsn files if available

Disk

- Collect all .vmdk files associated with the current snapshot ID

- Alternatively, create a single VMDK from split files:
C:\Program Files (x86)\VMware\VMware Player\vm-ware-vdiskmanager.exe» -r «d:\VMLinux\vmd-kname.vmdk» -t 0 MyNewImage.vmdk

BlueCapeSecurity - Practical Windows Forensics
https://github.com/bluecapesecurity/PWF

Memory acquisition – planning

Fast artifact collection

- Prepare a batch script to acquire server information, process, network, and user activities

Full memory acquisition

- Require inserting and mounting USB storage to a physical server
- Require remote upload and execute forensic tool on the server
- Disable the energy-saving feature on the workstation

Memory acquisition – on-site problems

[REDACTED]

[REDACTED]

Attack scenario summary

[REDACTED]

Findings

[REDACTED]

Findings (cont.)

[REDACTED]

Active Directory hardening and recovery

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events

Windows Server Get started Failover clustering Management Identity and access Networking Troubleshooting Related products

Filter by title

- Best Practices for Securing Active Directory
  - Best Practices for Securing Active Directory
  - Executive Summary
  - Introduction
  - Avenues to compromise
  - Attractive Accounts for Credential Theft
  - Reducing the Active Directory attack Surface
  - Implementing Least-Privilege Administrative models
  - Implementing Secure Administrative Hosts
  - Securing Domain Controllers Against attack
  - Monitoring Active Directory for Signs of compromise
  - Audit Policy Recommendations
  - Planning for compromise
  - Maintaining a more Secure Environment

Learn / Windows Server /

Best Practices for Securing Active Directory

Article • 07/29/2021 • 9 contributors

Feedback

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This document provides a practitioner's perspective and contains a set of practical techniques to help IT executives protect an enterprise Active Directory environment. Active Directory plays a critical role in the IT infrastructure, and ensures the harmony and security of different network resources in a global, interconnected environment. The methods discussed are based largely on the Microsoft Information Security and Risk Management (ISRM) organization's experience, which is accountable for protecting the assets of Microsoft IT and other Microsoft Business Divisions, in addition to advising a selected number of Microsoft Global 500 customers.

- Executive Summary
- Introduction
- Avenues to Compromise

Best Practices for Securing Active Directory
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Microsoft 365 Security

Everything about Microsoft Security

M365 Advanced Hunting | Azure Sentinel | Azure Active Directory | KQL | Microsoft Identity | Windows OS | Jupyter Notebooks | About

Practical Compromise Recovery Guidance For Active Directory

Posted on April 27, 2021 | by m365guy | One comment

Today I'm going to blog about compromise recovery in an Active Directory forest. I've been blogging for a while and have read tons of stuff about Active Directory, but one thing has been missing. Which is how we can recover from an active attacker?

There hasn't been many articles or blog posts around recovering an AD forest. Sure, when you search on the internet. You probably end up with the one from Microsoft, which can be found here. However, it might lack the in-depth examples. This makes it (IMO) harder for admins to understand the necessary steps, that needs to be taken. In order to reduce further damage, when there is an live incident.

The goal of this blog post is to explain how to recover Active Directory from an active attack with minimal disruption. This is not an Active Directory Security Assessment, and no. We're also not going to cover attacks related to AD. Goal of this blog post is to ensure that our Tier-0 resources are protected from further compromise.

Practical Compromise Recovery Guidance For Active Directory
https://m365internals.com/2021/04/27/practical-compromise-recovery-guidance-for-active-directory/

Case #1: Lessons learned

- Evaluate the need for full memory acquisition
  - Explain when and why it is required or not required
- Ensure a safe and clean working environment
  - Scope of the compromise might not be limited to the server zone
- Consider alternative methods
  - Snapshot, duplicate, and conduct live analysis
- Prepare for the worst-case scenario

Case #2: Investigating banking trojan

Scenarios

- A bank's customer chatted with an attacker and has been tricked to install malware on their computer, amount of money has been transferred to an attacker's account
- The victim ran multiple antimalware tools on their machine, some artifacts have been deleted
- An infected machine has been shut down before the forensics team arrived at the scene

Remaining artifacts and limitations

Artifacts and supporting information

- Windows event log
- Web browser history
- Antimalware log
  - All quarantined files were encrypted
- Chat history log
  - All chats were encrypted
- Online banking activity log
  - Provided by the victim’s bank

Findings

[REDACTED]

Decrypting the encrypted files

Where is the key?

- Quarantined malware files -> Unlock via Windows account password
- Chat history log -> Unlock via viewing with the chat app

Booting up the machine

- Restore the disk image to another hard drive and then boot it from an original machine
- Convert a raw disk image to a VM disk and then start the VM

Converting a raw image to a VM disk

Converting between image formats

Converting images from one format to another is generally straightforward.

qemu-img convert: raw, qcow2, qed, vdi, vmdk, vhd

The **qemu-img convert** command can do conversion between multiple formats, including **`qcow2`**, **`qed`**, **`raw`**, **`vdi`**, **`vhd`**, and **`vmdk`**.

qemu-img format strings

Image format	Argument to qemu-img
QCOW2 (KVM, Xen)	**`qcow2`**
QED (KVM)	**`qed`**
raw	**`raw`**
VDI (VirtualBox)	**`vdi`**
VHD (Hyper-V)	**`vpc`**
VMDK (VMware)	**`vmdk`**

This example will convert a raw image file named **`image.img`** to a qcow2 image file.

```
$ qemu-img convert -f raw -O qcow2 image.img image.qcow2
```

Run the following command to convert a vmdk image file to a raw image file.

```
$ qemu-img convert -f vmdk -O raw image.vmdk image.img
```

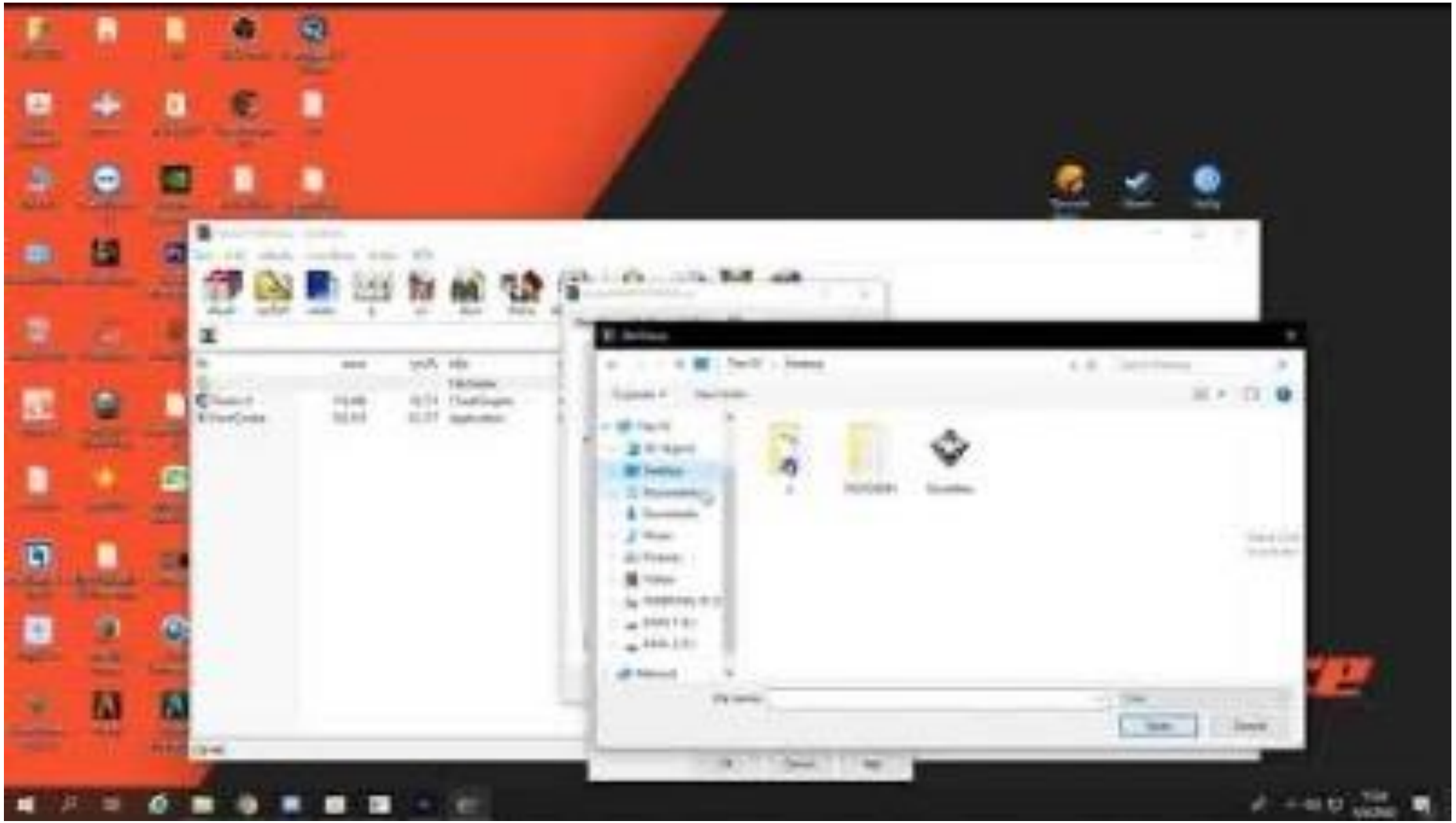
Run the following command to convert a vmdk image file to a qcow2 image file.

```
$ qemu-img convert -f vmdk -O qcow2 image.vmdk image.qcow2
```

OpenStack - Converting between image formats
https://docs.openstack.org/image-guide/convert-images.html

Findings (cont.)

[REDACTED]



njRAT
https://www.youtube.com/watch?v=nxnPkTubdNQ

Follow the traces

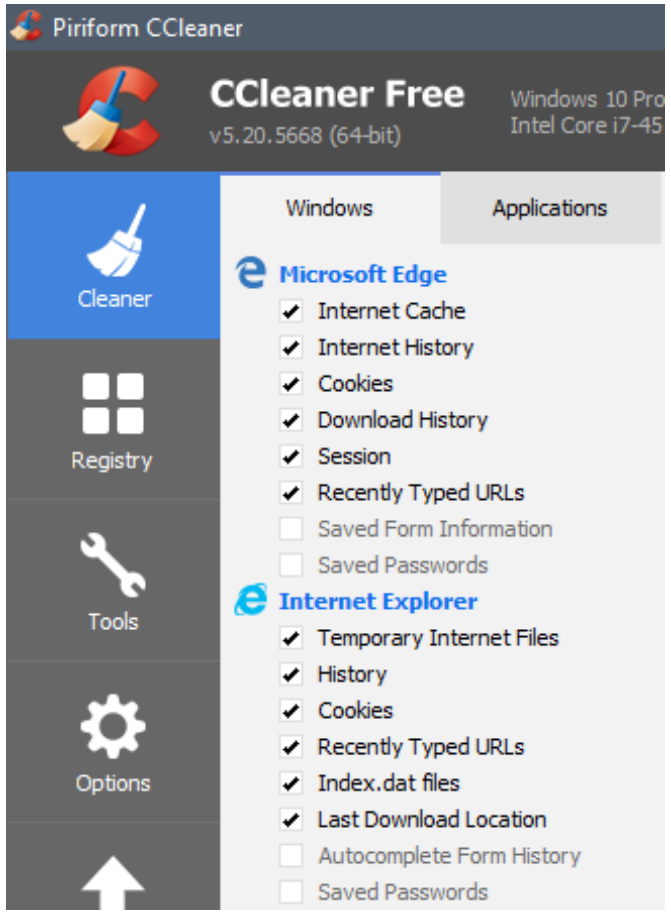
What have we known about the suspect

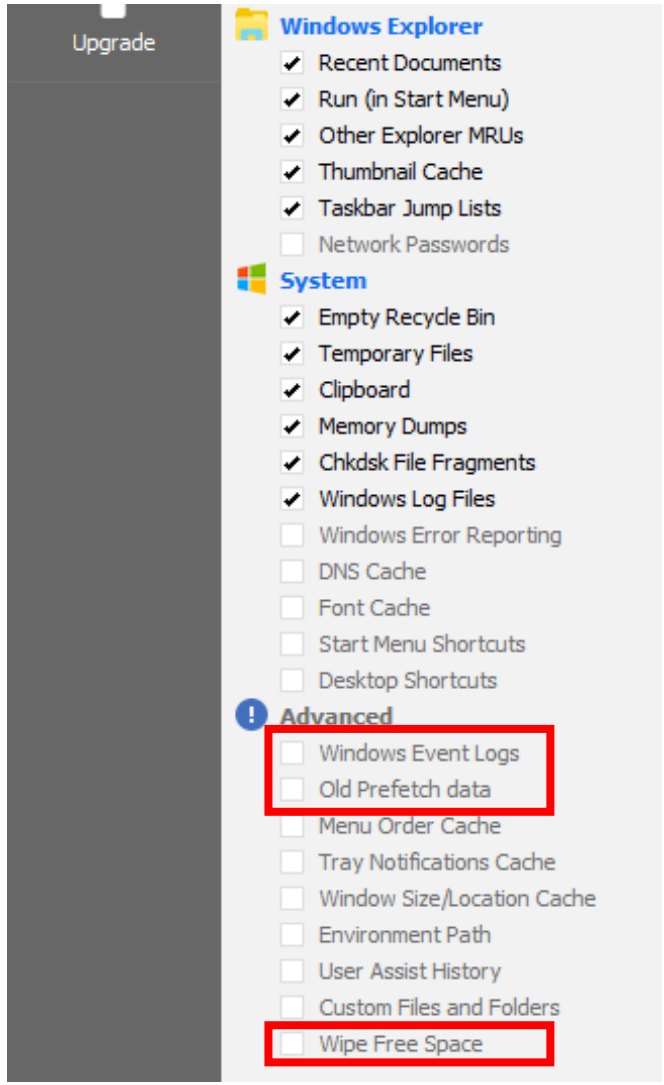
- Domain and IP of the C2 server
- IP of the chat user account
- Destination bank account
- etc.

Analyzing the suspected machines

[REDACTED]

Using CCleaner as an anti-forensic tool





CCleaner forensics
https://www.synacktiv.com/en/publications/ccleaner-forensics

Sample victim’s data in the suspected machine

[REDACTED]

Case #2: Lessons learned

- Remediation actions might affect forensic capabilities
  - Important data could be lost
- Learn more about the limitations of anti-forensic tools
  - Some privacy cleaner tools can be used to wipe attacker's traces
  - Look for the places that might contain data in RAM

Questions?

Thank you