Forensics for System Administrators

Organisation

Klaus Möller

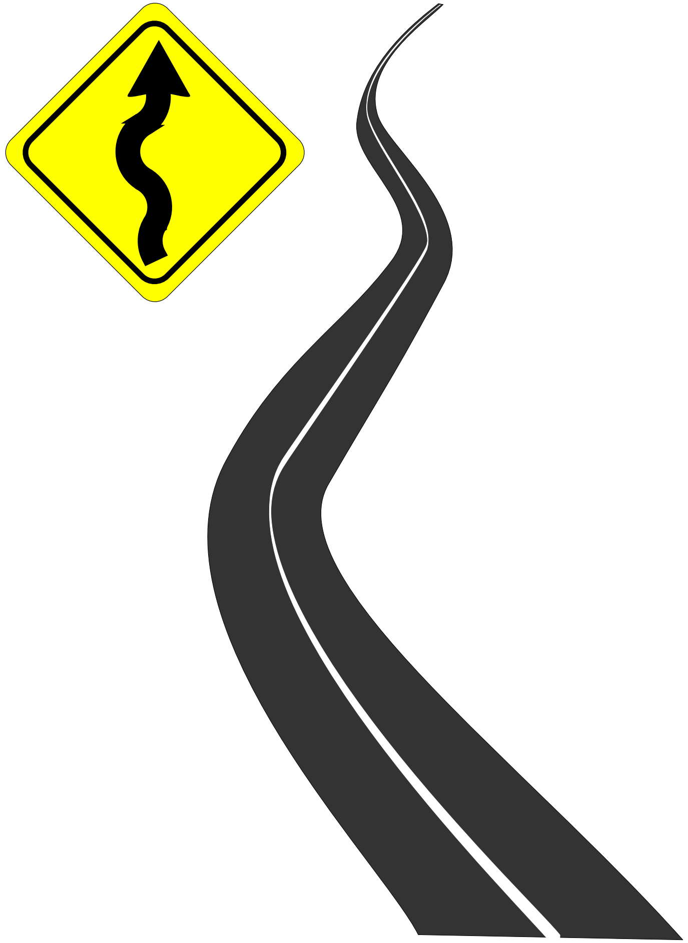
WP8-T1

Webinar, 23rd of November 2021

Public

www.geant.org

Agenda



- Motivation
- Incident Response Workflow
  - Preparation
  - Detection & analysis
  - Containment, eradication & recovery
  - Post-incident activity, lessons learnt
- Forensics Workflow
  - Operational Preparation/
  - Identification/Preservation
  - Collection
  - Processing
  - Review/Examination
  - Analysis
  - Reporting/Production
- Forensic Principles

Why forensic investigations are not concluded

- Paperwork? - *“I solve problems, I do not administer them”*
- No time for *“involved”* incident response/forensics
- No budget (for tools, training, effort, etc.)
- Lack of forensic tools
- Lack of knowledge
- *“We don’t get them anyway“*

Why do forensic investigations?

- Uncoordinated responses will be less effective or counterproductive
  - Evidence might be destroyed or made inadmissible
  - Traces might be overlooked
- Legal/regulatory requirements
  - E.g. ISO 27xxx or other certification
- Forensic knowledge can be applied to other areas of sysadmins work
  - Operational troubleshooting
  - Log monitoring
  - Data recovery/cloning
- Overlap with Business Continuity Management (BCM)
  - A lot of the paperwork/preparation can be reused
- Last, but not least: Training for incidents/forensics can be fun

Legal Disclaimer

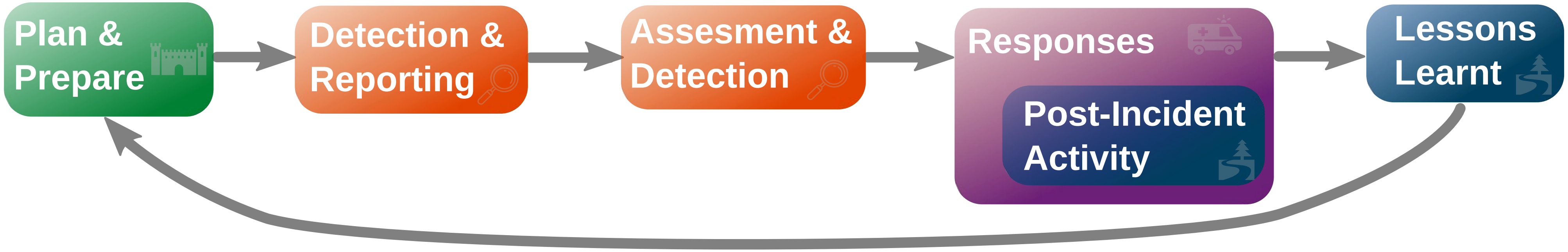
- We are not lawyers
  - Therefore, this will be technical/organisational advice only
- I.e. we are not qualified (or allowed) to give legal advice
  - German law explicitly forbids non-lawyers to give legal advice
  - Besides, covering the laws of over 30 countries (in Europe alone) is well beyond our capabilities
- Of course, you will need some
  - Criminal code, criminal proceedings code, workplace law, privacy protection law, etc.
  - Don’t forget your data/privacy protection officer/ombudsperson, etc.
- Sincerely, check with your legal counsel!
  - Otherwise, you’ll end up in a quagmire

Incident Response Workflow

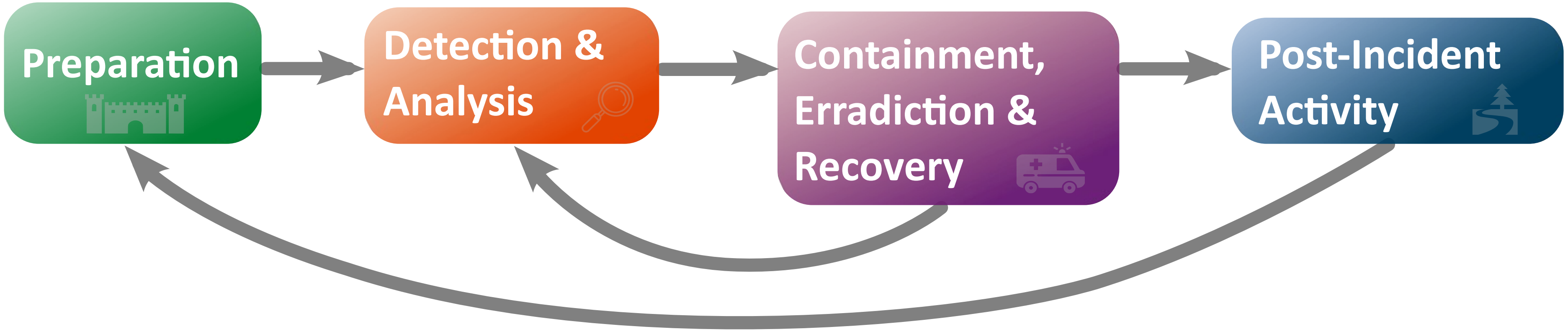
www.geant.org

Incident Response Workflow

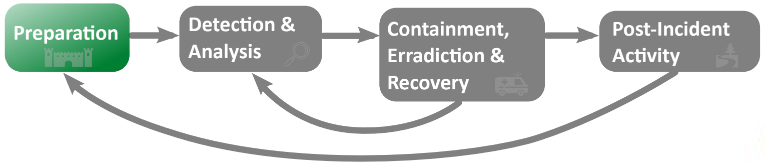
ISO/IEC 27035-1:2016



US NIST SP 800-61 rev 2



Incident Response: Preparation



Preparation

Detection & Analysis

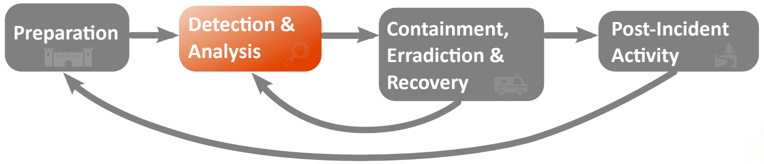
Containment, Erradiction & Recovery

Post-Incident Activity

- Documentation
  - Contact lists, phone numbers, etc.
  - HW-/SW-configuration, system location, keys for rooms, …
- Know how to use your Analysis-Tools & have them ready
- Workflows for Standard-Incidents/Exercises
- Resources: Personnel, Hardware, Rooms, etc.
- **The plan has to work when most of your infrastructure is down!**
- **Goal:** Having a plan
- **Advantages:**
  - Save time and money
  - Stress reduction
  - *Making an impact*

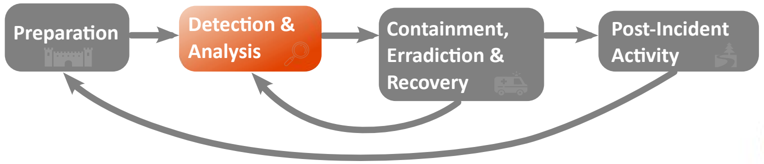
Preparation for forensics happens here too

Incident Response: Detection



- First:
  - Automated examination (of system states)
    - From your system/network management system, SIEM, etc.
    - Threat intelligence feeds, automated external alarm messages
  - Timely alerts
    - Yes, you need to watch your logs/alarms!
  - Receipt of manually incoming alerts
    - Your users/partners will be a vital source of information
- Building upon this:
  - Systematic search for traces
  - Documentation of all findings and suspicious facts
    - What tipped you off?
- **Goal:** To know whether there is really a security incident or not!

Incident Response: Analysis

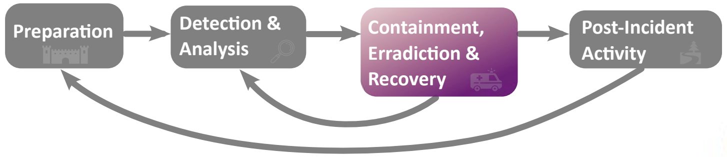


- **What?** - Assess damage done
- **How?** - Exploited vulnerabilities/weaknesses, ...
- **When?** - Timeline of events, resulting potential damage, ...
- **Who?** - Other affected parties, attackers

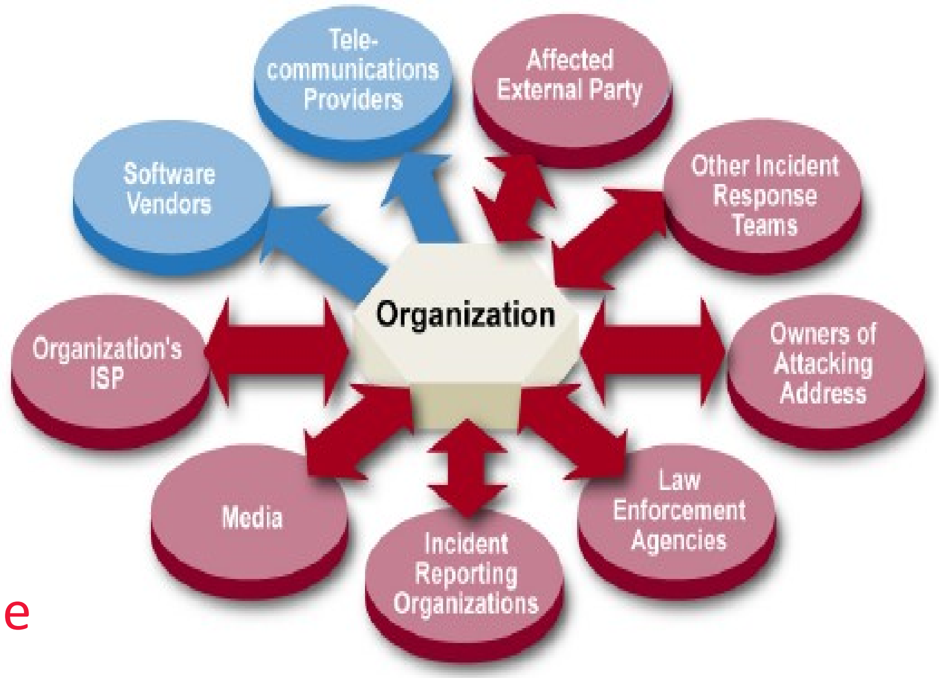
- **Goal:**
  - Input for the next phase
  - Prioritizing (Triage): Which incidents have precedence?

Here is, where forensics come into play

Incident Response: Containment

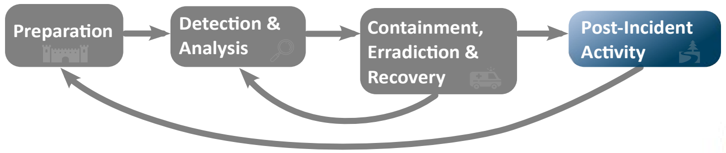


- **Short term goal:** Minimize the damage from the incident
- Coordination with 3rd parties
- Re-installation of systems
- Ad-hoc provisions & adaption of security measures


Organization
Software Vendors
Tele-communications Providers
Affected External Party
Other Incident Response Teams
Owners of Attacking Address
Law Enforcement Agencies
Incident Reporting Organizations
Media
Organization's ISP

- **Long term goal:** The attackers are definitely removed from the system
  - And they can not come back through the same hole

Incident Response: Post-Incident Activity



- Meeting with all actors
  - Processing of the facts as far as known
  - Final report of the incident
  - Praise and acknowledgment of the work done
- Documentation & dissemination of „*lessons learned*“
- Adjustment of the incident handling/forensics process
- Correction of identified gaps and problems
- **Goal:** Be better/really prepared next time!

After (one) the incident is before the (next) incident

So yes, it is really an Incident

- You have been hacked - now what?
- **Don’t Panic!** (yes, seriously)
- Follow the agreed upon plan (if you have one)
  - Do not fuss around
  - Undirected, unsystematic approach will destroy traces
- Coordinate
  - Colleagues, Leaders, Customers, etc.
- Take your time
  - Incidents happen 15 minutes before closing time, Friday
- Do not do the attackers work
  - Like disconnecting the network during a DDoS attack

Decision Point - Where do you want to go?

- Legal route - I.e. you want to take things to court
  - You think, your case/evidence will be good enough
  - Or you're required to take legal action
  - Let the investigation be done by trained forensics experts, preferably from law enforcement
  - However, most of this course will not be suitable for you
- Alternative route - Do not involve law enforcement, because
  - Data will not be good enough to stand up in court
  - Too much effort for a (small) incident
  - Do not see a chance to catch the culprits
  - **Main goal: Go back into secure service as soon as possible**

Forensics: “Quick and Dirty” (Leif Nixon)

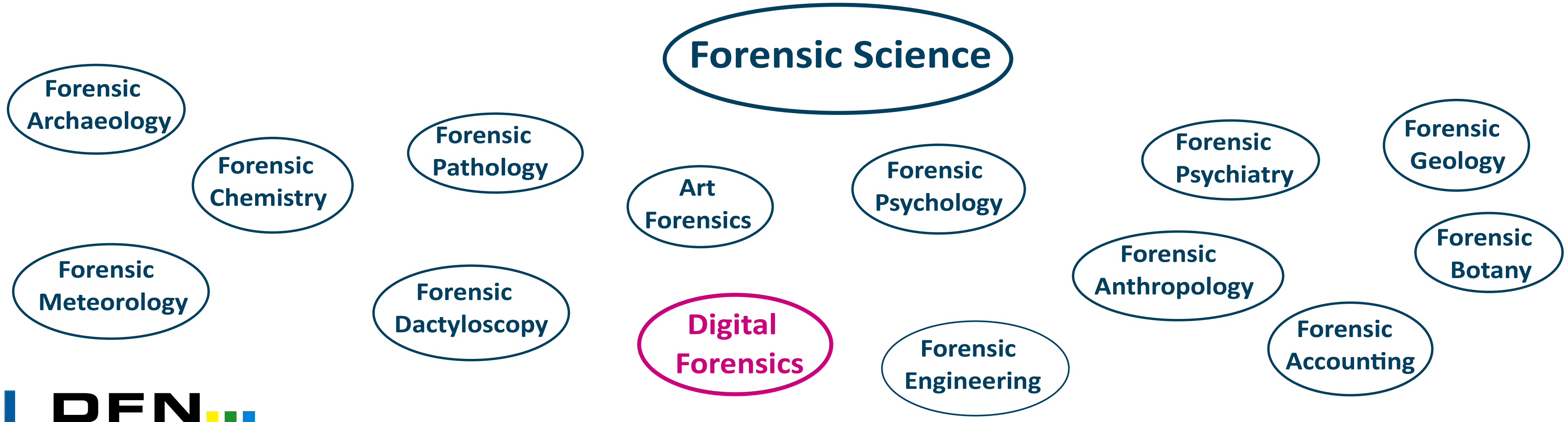
- Re-install the system and forget about the incident?
- No!
  - There might be backdoors left - intruders will come back
  - You might get re-infected - by the same intruders or others
- To get back into secure service you would like to know:
  - How the intruders got in?
  - When they did so?
  - What they have been doing on the system?
  - What we can do to stop them from returning?
  - Which other sites may have been hit?

Forensic Workflow

www.geant.org

Definition

- ***Forensics*** - short for ***Forensic Science***
  - Sometimes called ***Criminalistics***
- From Latin *forēnsis* - “of/before the Forum” (court place in ancient Rome)
- *“ … the application of science to criminal and civil laws, […] during [a] criminal investigation …”*
- A forensic scientist/investigator *“**collects, preserves,** and **analyses** scientific evidence during the course of an investigation”*



Forensic Science

Forensic Archaeology

Forensic Chemistry

Forensic Pathology

Art Forensics

Forensic Psychology

Forensic Psychiatry

Forensic Geology

Forensic Meteorology

Forensic Dactyloscopy

Digital Forensics

Forensic Engineering

Forensic Anthropology

Forensic Botany

Forensic Accounting

Terminology

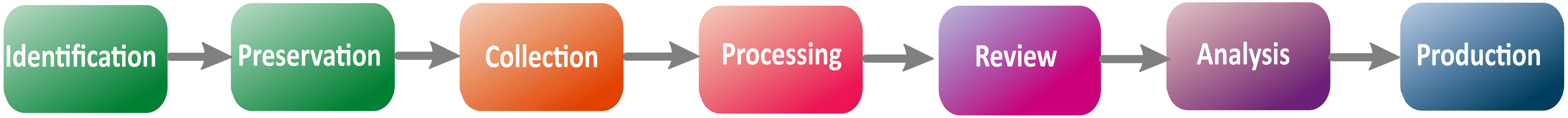
- ***Electronically Stored Information (ESI)***
  - In essence forensic traces in the form of digital data
- ***eDiscovery***
  - The process of acquiring and searching ESI for traces
- ***Electronic Evidence***
  - Evidence that is stored electronically/digitally
  - As opposed to other types of evidence: documents, physical evidence, testimonies, …
  - Evidence is what is used to establish *facts* in court cases

Characteristics of ESI

- **Invisible to the untrained eye**
  - I.e. it is often retrieved from places known or accessible only to experts
- **May need to be interpreted by a specialist**
  - Analysis and presentation required to be valid from a judicial point of view
- **Highly volatile / may be altered or destroyed through normal use**
  - System state changes constantly with each event → Deleted or old data will be overwritten
  - When powered off, volatile state (memory contents) may/will be lost
  - Use of appropriate tools and techniques from the moment of identification
- **Can be copied without limits**
  - Many specialists may work on their copies of the same information at the same time in different places
  - Possibility to present the evidence as-is in the court along with the specialist witness report

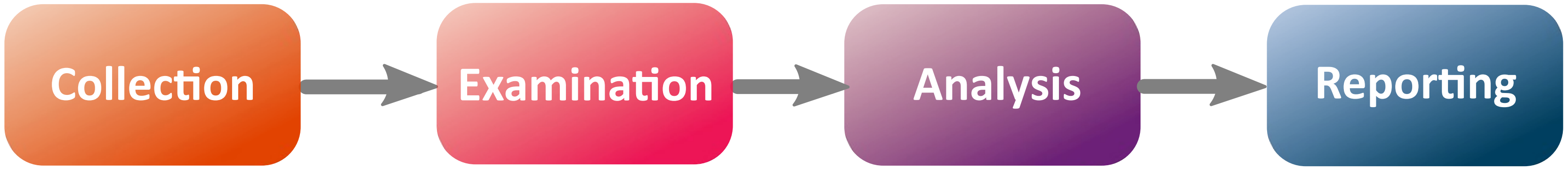
Forensic Workflow

ISO/IEC 27050:2016-2020



Identification → Preservation → Collection → Processing → Review → Analysis → Production

US NIST SP 800-86



Collection → Examination → Analysis → Reporting

Strategic Preparation

- Part of the preparation phase of incident response
- Definition of the (forensic) process
  - Roles and responsibilities
  - Information flow
  - Fitting/alignment with other policies (ISO 270xx, …)
- Selection and purchase of hard- and software
- Securing of other resources
- Approval/buy in from management
- Training

Operational Preparation

- Setting the scope of the forensic investigation
  - What is the goal of the investigation?
    - I.e. *„what do we want to find out?“*
    - Phrasing of questions of the investigation
  - What shall be examined?
- Example: Newly bought USB-stick was inserted into an infected system
  - Q1: Is there (now) malware on the Stick?
  - Q2: What kind/type of malware is it?
    - How does it spread (media, network)?
    - What does it do?
  - Q3: Is there any data/software/malware on the stick?

Identification/Preservation

- Selection of the ESI to be collected
  - What? - Hard disks, memory, NetFlows, logfiles, etc.
    - Further narrowing to relevant information: time-frame, users, etc.
    - Privacy protection, does certain information need to be excluded?
  - Where is it? - Location of systems, media, etc.
  - How much is it? - I. e. size
- Preservation
  - Putting ESI on legal hold (*freeze*)
  - Assuring that the ESI is not deleted, altered, or substituted
  - This will include non-disclosure of the ongoing investigation to others
- Priority - what to collect first
  - By order of volatility

Volatility of ESI

More volatile

Item	Avg. lifetime
Registers	Nanoseconds
Cache lines	
Processes	Seconds - Minutes
Sockets	Seconds - minutes
Open files	
Active Users	Minutes - Hours
Network configuration	
Registry (or other system config. DB)	
Files (closed)	Hours - Days
Unused blocks	
Slack space	
Partitions	
Hard disks	Months

Live response

- Data usually lives in main memory
- Will be lost on reboot/ power-off
- Or lost when pulling the plug from the network (timeouts)

Post mortem analysis

- Data in non-volatile storage
- Survives reboots
  - Caveat: Filesystems in main memory do not survive reboots

Collection

- Actually obtaining the ESI/securing the data
  - Output from tools
  - Image-creation (memory, storage media) as bit-by-bit copies
  - Logs, NetFlows, Packet-Captures, etc.
- Surrounding conditions
  - Change system state as little as possible
  - Put as little ***trust*** as possible in a (compromised) System
    - Malware might have altered information or lie about system state
- Document what you have been doing
  - By whom, when, where, and where the collected data is kept

Decision point - Live response or post mortem

- Not really an “*either … or …*” decision, but important for incident response

Live respnse	Isolating/powering-off the system
Might obtain volatile information that would otherwise be lost	Will lose volatile data
Investigators actions might tip of the intruder	Might also tip off the attacker (if intruder installed a dead-man switch)
Intruder can do further damage when opting to observe its behaviour	Will prevent further damage (to other systems)

Processing

- Collected data is imported into the forensic tools
  - To enable searching and analysing
  - Extraction of pictures, videos, office documents, etc.
  - Reconstruction/extraction of deleted files
- Filtering out unneeded data/information
- Normalisation of different data formats (e.g. timestamps)
  - Different clock settings have to be taken into account
    - Time zones, summer/winter time, non synchronized clocks
- Building of a (super) Timeline
  - For chronological searches
  - To visualize the chronological sequence of events (for reports)

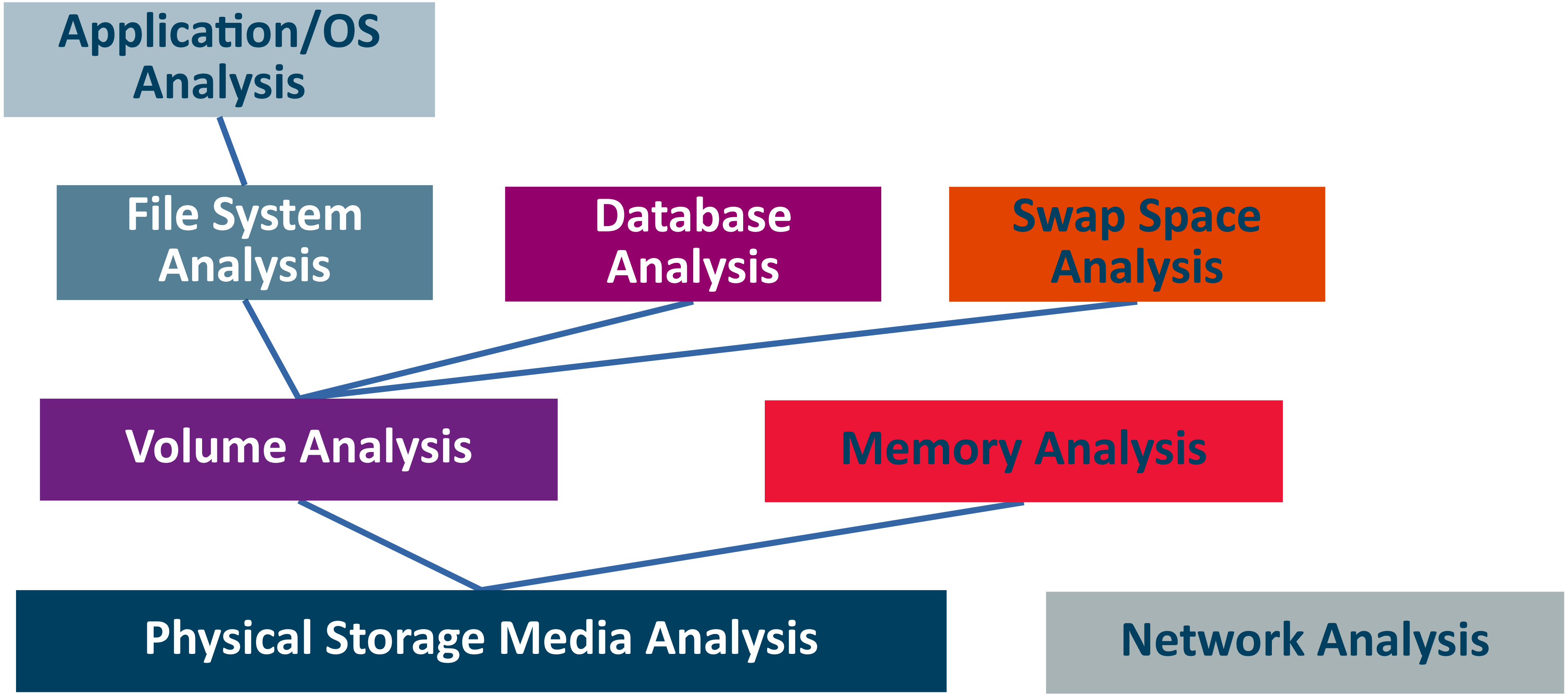
Review/Examination

- Assessment of the collected data
- Starting point: Questions from operational preparation
- Breaking down questions until these can be answered directly from the data (*divide and conquer*)
- Search for *Indicators Of Compromise* (IOC)s
  - Artefacts that may point to the compromise of a system
  - E.g. the checksum of a file matches that of a known malware, new accounts, etc.

Analysis

- Drawing conclusions from examined data
- Care has to be taken as
  - Data from compromised systems will (very likely) be forged
  - Data will (most probably) be incomplete
  - *„Everything is hearsay“* unless proven from independent, trustworthy sources
- Results will always have a certain degree of uncertainness
  - Hence a compromise can not be ruled out, even if all results are negative
  - More data might have to be collected → back to Collection step

Analysis Objects



Application/OS Analysis

File System Analysis

Database Analysis

Swap Space Analysis

Volume Analysis

Memory Analysis

Physical Storage Media Analysis

Network Analysis

Source: Brian Carrier: “File System Forensic Analysis”

Reporting/Production

- Presentation of results for corresponding target groups
  - Special case: Presentation at court of law
  - Usually along with the original evidence (i.e. hard disks, laptops, etc.)
- Timelines or other visualizations
- „Executive Summary“ for management (non-techies)
- Comprehensive report with detailed description of examination and analysis steps taken, problems, questions, etc. (techies)
- Recommendations for further proceedings (optional)
  - As input for next phases of incident response and lessons learned
  - Or as general recommendations to improve security

Forensic Principles

- Laws regarding admissibility of evidence differ between countries
- Hence, the EU and the Council of Europe (COE) founded a project for a *seizure of e-evidence* guide
  - *Electronic evidence guide, v. 1.0*, created as part of CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime
- Five principles were identified that are commonly used internationally

Data Integrity

Audit trail

Specialist support

Training

Legality

Data Integrity

- No action taken should change electronic devices or media, which may subsequently be relied upon in court
  - When handling electronic devices and data, they must not be changed, either in relation to hardware or software
  - The person in charge is responsible for the integrity of the material recovered from the scene and thus for initiating a forensic chain of custody
  - There are circumstances where a decision will be made to access the data on a 'live' computer system to avoid the loss of potential evidence.
  - This must be undertaken in a manner which causes the least impact on the data and by a person qualified to do so

Audit Trail

- An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved
  - Can be in paper form or electronically
  - As long as it is admissible at court
- An independent third party should be able to examine those actions and achieve the same result
- Other term: ***Chain of Custody***
- *What happens when the chain of custody is broken or absent?*
- Answer: *Depends on the countrys legal system*

Example Chain of Custody Recording

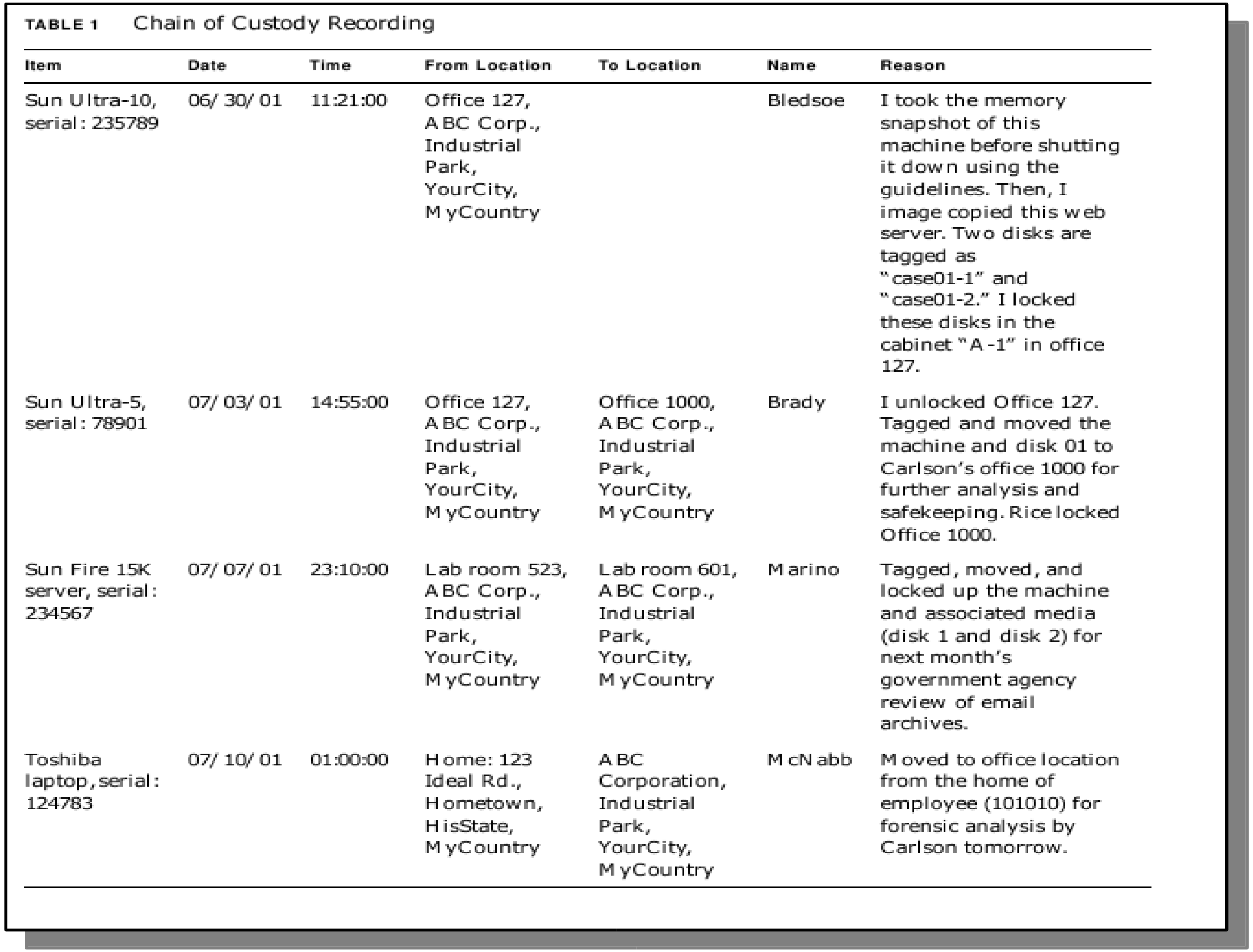
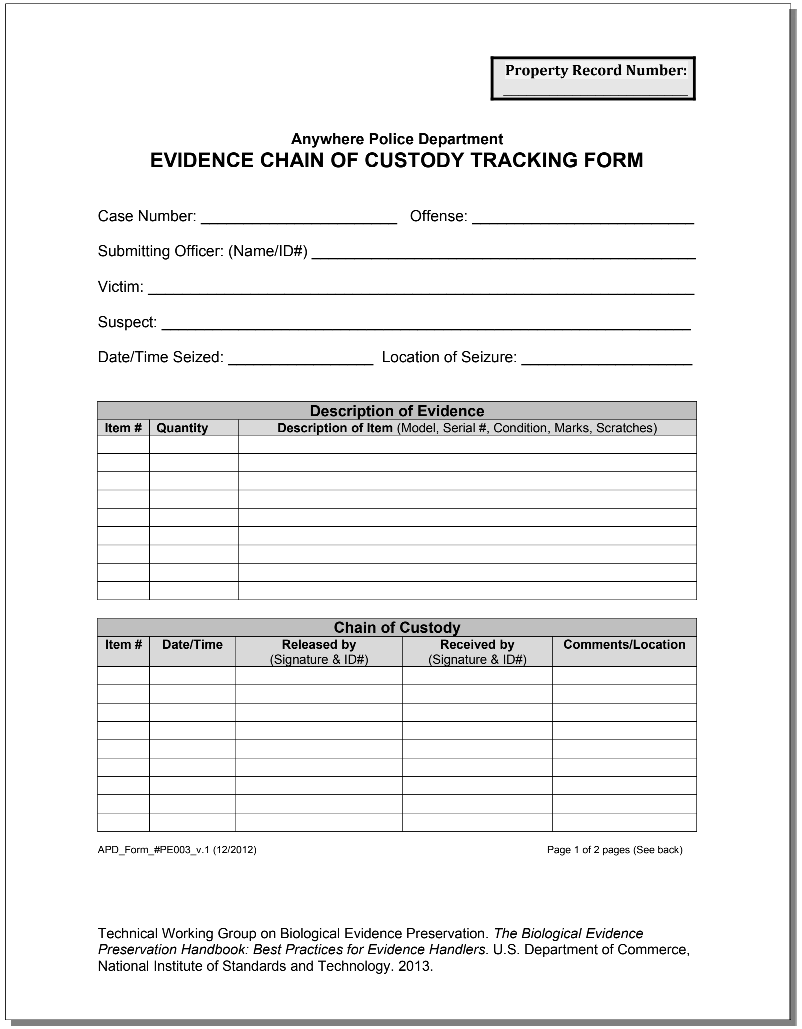


TABLE 1 Chain of Custody Recording

Item	Date	Time	From Location	To Location	Name	Reason
Sun Ultra-10, serial: 235789	06/30/01	11:21:00	Office 127, ABC Corp., Industrial Park, YourCity, MyCountry		Bledsoe	I took the memory snapshot of this machine before shutting it down using the guidelines. Then, I image copied this web server. Two disks are tagged as "case01-1" and "case01-2." I locked these disks in the cabinet "A-1" in office 127.
Sun Ultra-5, serial: 78901	07/03/01	14:55:00	Office 127, ABC Corp., Industrial Park, YourCity, MyCountry	Office 1000, ABC Corp., Industrial Park, YourCity, MyCountry	Brady	I unlocked Office 127. Tagged and moved the machine and disk 01 to Carlson's office 1000 for further analysis and safekeeping. Rice locked Office 1000.
Sun Fire 15K server, serial: 234567	07/07/01	23:10:00	Lab room 523, ABC Corp., Industrial Park, YourCity, MyCountry	Lab room 601, ABC Corp., Industrial Park, YourCity, MyCountry	Marino	Tagged, moved, and locked up the machine and associated media (disk 1 and disk 2) for next month's government agency review of email archives.
Toshiba laptop, serial: 124783	07/10/01	01:00:00	Home: 123 Ideal Rd., Hometown, HisState, MyCountry	ABC Corporation, Industrial Park, YourCity, MyCountry	McNabb	Moved to office location from the home of employee (101010) for forensic analysis by Carlson tomorrow.

Source: "Responding to a Customer's Security Incidents — Part 4: Processing Incident Data" Sun BluePrints™ OnLine, October 2003

Example Chain of Custody Form



Property Record Number: ____________

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: ______________________ Offense: _________________________

Submitting Officer: (Name/ID#) ____

Victim: ____

Suspect: ____

Date/Time Seized: ________________ Location of Seizure: ___________________

Description of Evidence

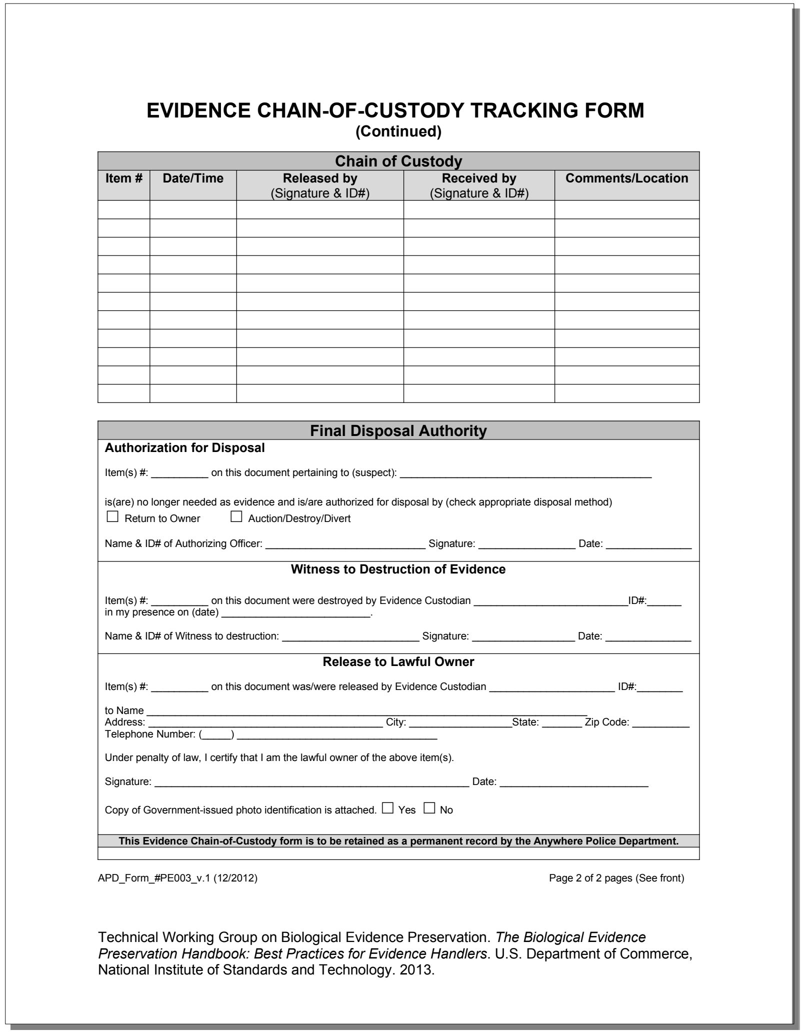
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.



EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

(Continued)

Chain of Custody

Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Authorization for Disposal

Item(s) #: __________ on this document pertaining to (suspect): ____

is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
□ Return to Owner □ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: ____________________________ Signature: _________________ Date: _______________

Witness to Destruction of Evidence

Item(s) #: __________ on this document were destroyed by Evidence Custodian ___________________________ID#:______
in my presence on (date) __________________________.

Name & ID# of Witness to destruction: ________________________ Signature: __________________ Date: _______________

Release to Lawful Owner

Item(s) #: __________ on this document was/were released by Evidence Custodian ______________________ ID#:________

to Name ____
Address: ____ City: __________________State: _______ Zip Code: __________
Telephone Number: (_____) ___________________________________

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: ____ Date: __________________________

Copy of Government-issued photo identification is attached. □ Yes □ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Wrapping Up

www.geant.org

What have you learned?

- Basic workflow of Incident Response & Forensics
  - Prepare
  - Plan your investigation, i. e.
    - What do you want to know?
    - Where is the information to answer these questions?
  - Collect Electronically Stored Information (ESI)
    - This is, where the rest of the module focusses upon
  - Examine & Analyse
    - Take care of integrity and audit trail (forensic principles)
  - Report your findings

Thank you

Any questions?

Next Webinar: ***From Suspicion to Detection***

November 30th, 2021

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

References: Incident Handling Standards

- US NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide (2012), https://doi.org/10.6028/NIST.SP.800-61r2
- ENISA
  - *Good Practice Guide for Incident Management*, 2010, `https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management`
- ISO/IEC 27035:2016+ Information security incident management
  - ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
  - ISO/IEC 27035-2:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response
  - ISO/IEC 27035-3:2020 Information security incident management — Part 3: Guidelines for ICT incident response operations
  - ISO/IEC 27035-4 Information security incident management — Part 4: Coordination (DRAFT)

References: Forensic Standards

- US NIST Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response*, 2006, `https://doi.org/10.6028/NIST.SP.800-86`
- US NIST Special Publication 800-101 rev 1 *Guidelines on Mobile Device Forensics*, 2014, `https://doi.org/10.6028/NIST.SP.800-101r1`
- ISO/IEC 27037:2012 *Guidelines for identification, collection, acquisition and preservation of digital evidence*
- ISO/IEC 27041:2015 *Guidance on assuring suitability and adequacy of incident investigative method*
- ISO/IEC 27042:2015 *Guidelines for the analysis and interpretation of digital evidence*
- ISO/IEC 27043:2015 *Incident investigation principles and processes*
- ISO/IEC 27050:2018-2021 *Electronic discovery*
  - ISO/IEC 27050-1:2019 *Electronic discovery — Part 1: Overview and concepts*
  - ISO/IEC 27050-2:2018 *Electronic discovery — Part 2: Guidance for governance and management of electronic discovery*
  - ISO/IEC 27050-3:2020 *Electronic discovery — Part 3: Code of practice for electronic discovery*
  - ISO/IEC 27050-4:2021 *Electronic discovery — Part 4: Technical readiness*

Sample Forensic Distributions

- SIFT (SANS Investigative Forensic Toolkit): https://www.sans.org/tools/sift-workstation/
- CAINE (Computer Aided Investigative Environment): https://www.caine-live.net/
- GRML Forensic: https://grml-forensic.org/
- ALT Linux Rescue: https://en.altlinux.org/Rescue
- BlackArch: https://blackarch.org/
- BackBox: https://www.backbox.org/
- KALI (formerly Backtrack): https://www.kali.org/downloads/
- Matriux: http://www.matriux.com/
- Safe Boot Disk (Windows based): https://www.forensicsoft.com/help/SAFE_Boot1-1/