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
Incident Response Workflow

ISO/IEC 27035-1:2016

US NIST SP 800-61 rev 2
Incident Response: Preparation

- 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

- **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!
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
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”
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

US NIST SP 800-86
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
    • 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

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

**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

<table>
<thead>
<tr>
<th>Live response</th>
<th>Isolating/powering-off the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Might obtain volatile information that would otherwise be lost</td>
<td>Will lose volatile data</td>
</tr>
<tr>
<td>Investigators actions might tip of the intruder</td>
<td>Might also tip off the attacker (if intruder installed a dead-man switch)</td>
</tr>
<tr>
<td>Intruder can do further damage when opting to observe its behaviour</td>
<td>Will prevent further damage (to other systems)</td>
</tr>
</tbody>
</table>
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 uncertainty
  - 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 country’s legal system*
# Example Chain of Custody Recording

<table>
<thead>
<tr>
<th>Item</th>
<th>Date</th>
<th>Time</th>
<th>From Location</th>
<th>To Location</th>
<th>Name</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Ultra-20, serial: 2357939</td>
<td>06/30/01</td>
<td>11:21:00</td>
<td>Office 127, ABC Corp., Industrial Park, YourCity, MyCountry</td>
<td></td>
<td>Bledsoe</td>
<td>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 &quot;case01-1&quot; and &quot;case01-2.&quot; I locked these disks in the cabinet &quot;A-1&quot; in office 127.</td>
</tr>
<tr>
<td>Sun Ultra-S, serial: 769901</td>
<td>07/03/01</td>
<td>14:55:00</td>
<td>Office 127, ABC Corp., Industrial Park, YourCity, MyCountry</td>
<td>Office 1000, ABC Corp., Industrial Park, YourCity, MyCountry</td>
<td>Brady</td>
<td>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.</td>
</tr>
<tr>
<td>Sun Fire 1SK server, serial: 234567</td>
<td>07/07/01</td>
<td>23:30:00</td>
<td>Lab room S23, ABC Corp., Industrial Park, YourCity, MyCountry</td>
<td>Lab room 801, ABC Corp., Industrial Park, YourCity, MyCountry</td>
<td>Marino</td>
<td>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.</td>
</tr>
<tr>
<td>Toshiba laptop, serial: 124783</td>
<td>07/10/01</td>
<td>01:00:00</td>
<td>Home: 123 Ideal Rd., Hometown, HisState, MyCountry</td>
<td>ABC Corporation, Industrial Park, YourCity, MyCountry</td>
<td>McNabb</td>
<td>Moved to office location from the home of employee (101010) for forensic analysis by Carlson tomorrow.</td>
</tr>
</tbody>
</table>

Source: “Responding to a Customer’s Security Incidents — Part 4: Processing Incident Data” Sun BluePrints™ OnLine, October 2003
Example Chain of Custody Form

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

<table>
<thead>
<tr>
<th>Item #</th>
<th>Quantity</th>
<th>Description of Item (Model, Serial #, Condition, Marks, Scratches)</th>
</tr>
</thead>
</table>

Chain of Custody

<table>
<thead>
<tr>
<th>Item #</th>
<th>Date/Time</th>
<th>Released by</th>
<th>(Signature &amp; ID#)</th>
</tr>
</thead>
</table>

Final Disposal Authority

Authorization for Disposal

☐ 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.

Wrapping Up
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 30\(^{th}\), 2021*

[www.geant.org](http://www.geant.org)
References: Incident Handling Standards

- ENISA
- ISO/IEC 27035:2016+ Information security incident management
  - ISO/IEC 27035-4 Information security incident management — Part 4: Coordination (DRAFT)
References: Forensic Standards

- ISO/IEC 27041:2015 Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27043:2015 Incident investigation principles and processes
Sample Forensic Distributions

- 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/