# Steps for Analysing aquired data

## Case preparation

**Prepare evidence data from aquisition**

- What is this case about - short description
- Whos is responsible for the analysis?
- Time, date and prerequisites for the analysis
- How many pieces of evidence was analysed in this case?
- What software was used and version number (fx autopsy, EnCase, Magnet Axiom etc.)
- Is there any additional information that needs to be provided?
- IMPORTANT - NTP Timezone
- What hypothesis is there in regards to the case? and a quick overview of the hypothesises are sorrunding the case?

**Constraints - limitations**

If there are any boundaries to the case, this needs precise and short description

- Time limitation
- Specific search for a hypotheses or files/artefacts
- Use of a specific search towards the secured data (IOC, YARA, HASH, method of seach from vendor (File identification)
- SSD limitations - TRIM process can delete files under collection

**Analysis on evidence**

*This is not an exaustive list as this can get long. I have tried to put as much here as possible*

- Have malware been used ?
  - Any known identified files from Antimalware vendors
  - Have any IOC´s been used to test evidence?
  - Have there been checked for common actions, that malware perform?
    - New files spawned
    - Contact to malicious domaine /IP´s
    - Unusial activity to the user folder (exe file etc), Timeline activity that shows this
    - Download of files from the Internet
    - Schedueled tasks
- Have crafted scripts been in use?
  - Any signs of scripts been activated (Powershell scripts, DLL, python ect)
  - Any Priviledge escalation performed
  - Software installations performed with priviledged users?


L A R S B L O M G A A R D - K E A X L E B @ K E A . D K

# Steps for Analysing aquired data

**Analysis on evidence - continued**

*This is not an exaustive list as this can get long. I have tried to put as much here as possible*

- USB devices
  - How many external devices have been connected to the computer/evidence?
  - Model, make and serial number
- Memory analysis
  - Specify the actions you performed (Loaded DLL, DNS cache, Loaded devices, Command history, network connections, etc)
  - What software was used to perfom the analysis (fx Volatilty version 2 or 3?)
  - List the analysis queries performed and link to output
  - Short describe if the analysis gave the output / result that you expected
  - (Consider leave the above out, if the result did not deliver what was expected, and then write that in the report)
  - *SANS six-part methodology - Identify rogue processes, analyze processes and DLL, Network artefacts, Look for evidence of codeinjection, Signs of root kit and dump suspicious drivers and processes*
- Master File Table (MFT)
- Prefech file analysis
- Network cache
  - DNS cache
  - connections
- Browser data
  - Search history
  - cache analysis
  - known bad web domains / IP´s
  - download history
- E-mail
  - Phishing /Spearphishing attenpts
  - attemts of extraction of information, money transactions based on above
  - Files attached
  - Search of keywords (provide / describe the list used for searching for keywords, see keywords)
- Webshells
  - Why the seach of webshells. Are the system exposed to the Internet ? and how


L A R S B L O M G A A R D - K E A X L E B @ K E A . D K

# Steps for Analysing aquired data

**Analysis on evidence - continued**

*This is not an exaustive list as this can get long. I have tried to put as much here as possible*

- Pictures, videoes and media files
  - EXIF data
  - Size
  - Codecs
  - Known hash values for illegal cases (Make sure that the police are involved in these cases. If in doubt, BDO NOT CARRY OUT THE INVESTEGATION!!!)
  - Analysis for Steganography if suspicion is in place
  - calculate HASH values based on the files
  - Search constraints. Have the investegation only looked for file sizes, to narrow the search carried out
- Keyword search
  - What word list was used
  - How many words was searched for?
  - Why the sarch for these words? the meaning for the case?
- Timeline anslysis
  - What is the timeline for activity
  - Copy, move, creation, deletion, changes
- Filter searches
  - Does the tool support search for specific searches. Fx Autopsy use ingest modules, what modules was used?
  - **Can we dualtool verify these searches / results? IMPORTANT**
- Registry analysis
  - Analyse SAM, SECURITY, SOFTWARE, SYSTEM (from C:\Windows\System32\config)
  - HKEY_CURRENT_USERS
  - HKEY_USERS
  - HKEY_CLASSES_ROOT
  - HKEY_LOCAL_MACHINE
  - HKEY_CURRENT_CONFIG
- History (bash), commands fx curl, cp, chmod, sudo, ls, mv, grep, ps, tar, ftp, tftp, wget
- Event logs


L A R S B L O M G A A R D - K E A X L E B @ K E A . D K

# Steps for Analysing aquired data

**Report of output (Defined from the Governance / IT-security team in the company and Senion Mangement)**

- Document overview
  - Reference to ticket/incident /event
  - Quick info about the case
- Executive summary
  - Summary of events
  - graphic timeline
  - Root cause to incident
  - Highlevel reccomendations
- Abbreviations and list of definitions
- Incident Investegation report
  - What was the driver for the forensics investegation (Crime carried out, internal vilations to AUP)
  - Why was it a Crime? what is the illegal intent?
  - Network overview
  - Forensics analysis overview
  - Containemtn actions
  - Findings, root cause and artefacts
  - Remediation
  - Reccomendations
- Forensic report
  - Examiner and background
  - Tools used (versions and maybe known issues)
  - Tool Output
  - maybe utelization of dual tool verification
  - Collection method / Chain Of Custody
- Preparing the incident and forensic report
- Addendums

This needs to be defined before the incident and this needs to be acknowledged and accepted from C-level from the company


L A R S B L O M G A A R D - K E A X L E B @ K E A . D K