IT-SECURITY
ACTIONCARD -
FORENSICS ANALYSIS

Steps for aquire live 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
  - And later the time spendt on the evidence
- 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
- Pictures of the aquied setup

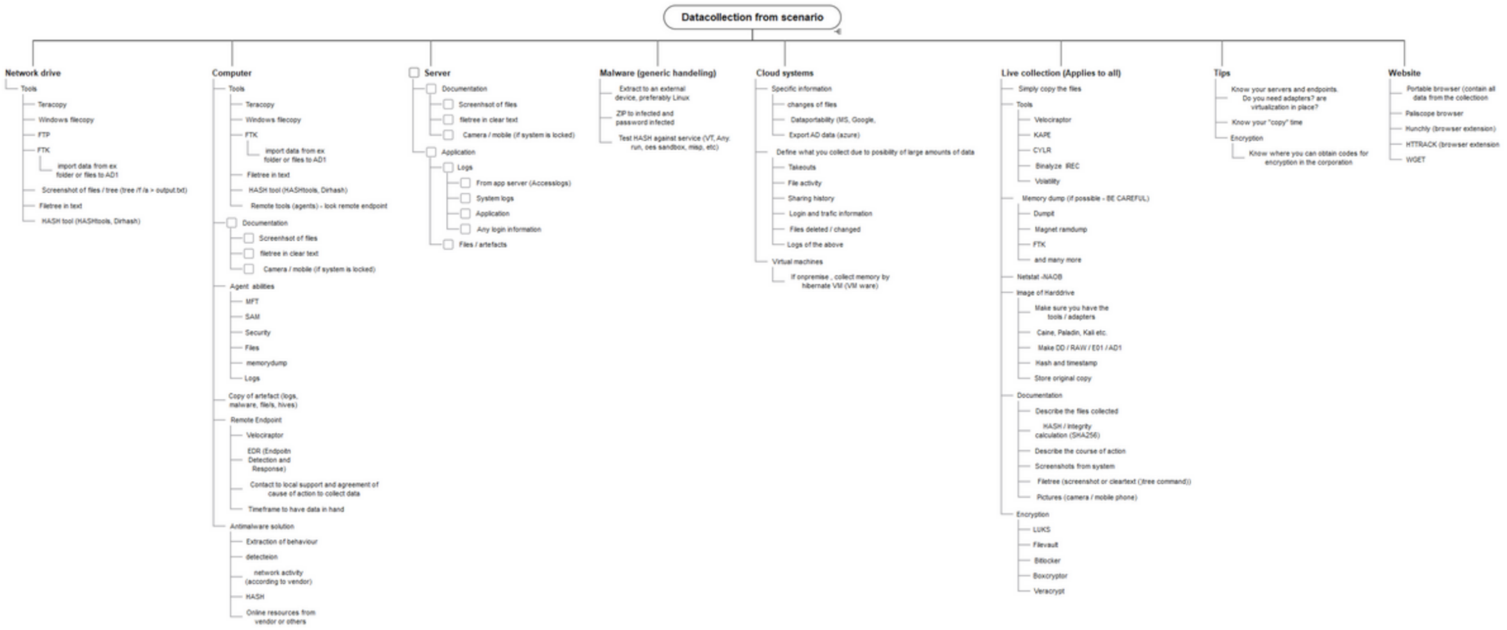
L**imitations**

If there are any boundaries to the case, this needs precise and short description
- Time limitation
- Physical limitations
- Circumstances that inhibits the full collection

Tools in toolbox
- Kape
- Memory tools, fx magnet ramdump, dumpit, FTK imager
- CyLR
- Velociraptor
- FTK imager for image aquisition

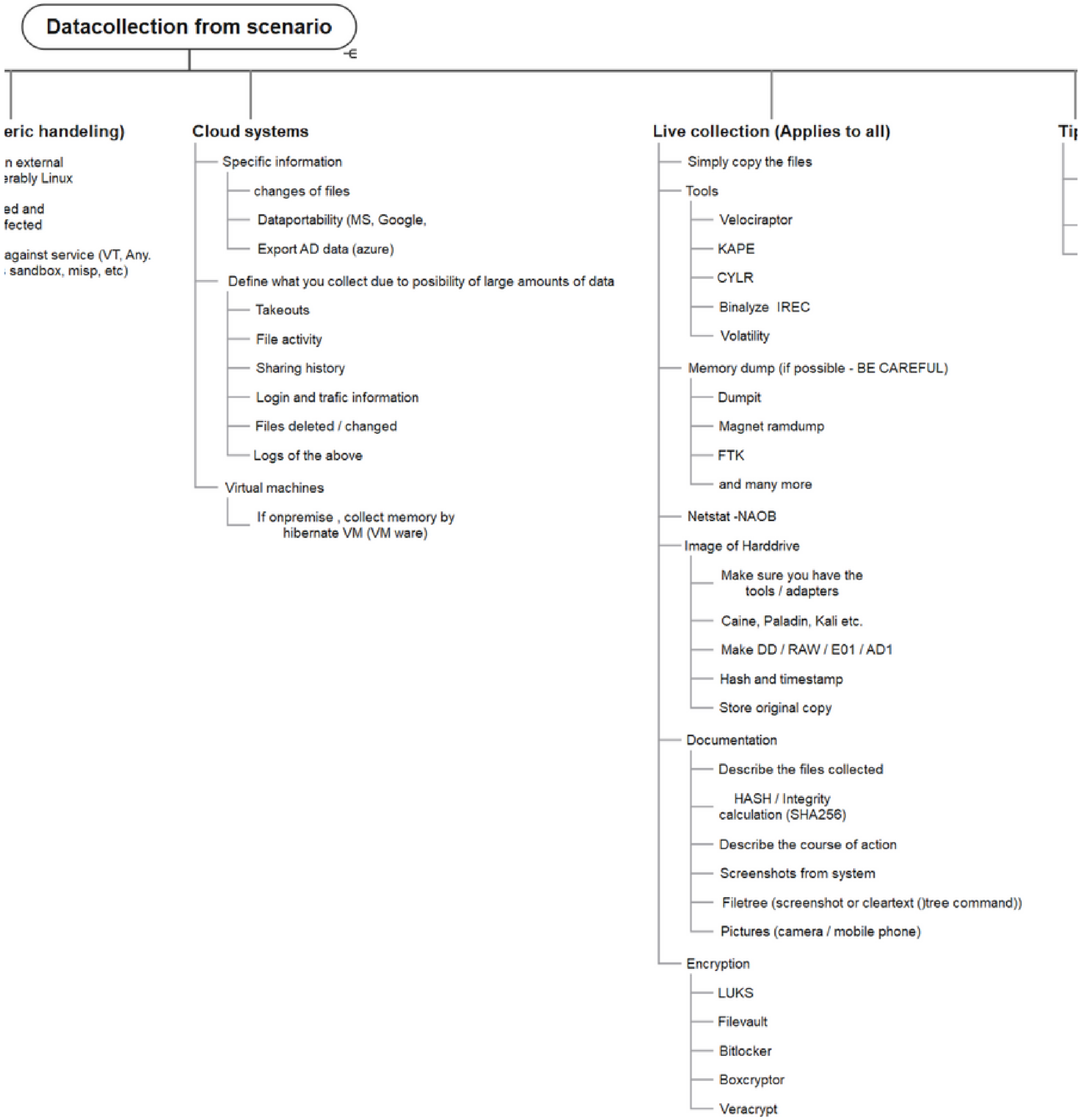
Analysis on evidence

This is not an exaustive list as this can get long. I have tried to put as much here as possible
- What tools was installed and run
  - Version
  - timeframe
  - and actions performed
  - Memory dump performed o not
- Commands used on the system



Datacollection from scenario

- Network drive
  - Tools
    - Teracopy
    - Windows filecopy
    - FTP
    - FTK
      - import data from ex folder or files to AD1
    - Screenshot of files / tree (tree /f /a > output.txt)
    - Filetree in text
    - HASH tool (HASHtools, Dirhash)
- Computer
  - Tools
    - Teracopy
    - Windows filecopy
    - FTK
      - import data from ex folder or files to AD1
    - Filetree in text
    - HASH tool (HASHtools, Dirhash)
    - Remote tools (agents) - look remote endpoint
  - □ Documentation
    - □ Screenhsot of files
    - □ filetree in clear text
    - □ Camera / mobile (if system is locked)
  - Agent abilities
    - MFT
    - SAM
    - Security
    - Files
    - memorydump
    - Logs
  - Copy of artefact (logs, malware, file/s, hives)
  - Remote Endpoint
    - Velociraptor
    - EDR (Endpoitn Detection and Response)
    - Contact to local support and agreement of cause of action to collect data
    - Timeframe to have data in hand
  - Antimalware solution
    - Extraction of behaviour
    - detecteion
    - network activity (according to vendor)
    - HASH
    - Online resources from vendor or others
- □ Server
  - □ Documentation
    - □ Screenhsot of files
    - □ filetree in clear text
    - □ Camera / mobile (if system is locked)
  - □ Application
    - □ Logs
      - □ From app server (Accesslogs)
      - □ System logs
      - □ Application
      - □ Any login information
    - □ Files / artefacts
- Malware (generic handeling)
  - Extract to an external device, preferably Linux
  - ZIP to infected and password infected
  - Test HASH against service (VT, Any. run, oes sandbox, misp, etc)
- Cloud systems
  - Specific information
    - changes of files
    - Dataportability (MS, Google,
    - Export AD data (azure)
  - Define what you collect due to posibility of large amounts of data
    - Takeouts
    - File activity
    - Sharing history
    - Login and trafic information
    - Files deleted / changed
    - Logs of the above
  - Virtual machines
    - If onpremise , collect memory by hibernate VM (VM ware)
- Live collection (Applies to all)
  - Simply copy the files
  - Tools
    - Velociraptor
    - KAPE
    - CYLR
    - Binalyze IREC
    - Volatility
  - Memory dump (if possible - BE CAREFUL)
    - Dumpit
    - Magnet ramdump
    - FTK
    - and many more
  - Netstat -NAOB
  - Image of Harddrive
    - Make sure you have the tools / adapters
    - Caine, Paladin, Kali etc.
    - Make DD / RAW / E01 / AD1
    - Hash and timestamp
    - Store original copy
  - Documentation
    - Describe the files collected
    - HASH / Integrity calculation (SHA256)
    - Describe the course of action
    - Screenshots from system
    - Filetree (screenshot or cleartext ()tree command))
    - Pictures (camera / mobile phone)
  - Encryption
    - LUKS
    - Filevault
    - Bitlocker
    - Boxcryptor
    - Veracrypt
- Tips
  - Know your servers and endpoints. Do you need adapters? are virtualization in place?
  - Know your "copy" time
  - Encryption
    - Know where you can obtain codes for encryption in the corporation
- Website
  - Portable browser (contain all data from the collectioon
  - Paliscope browser
  - Hunchly (browser extension)
  - HTTRACK (browser extension
  - WGET



Datacollection from scenario

- eric handeling)
  - n external
erably Linux
  - ed and
fected
  - against service (VT, Any.
; sandbox, misp, etc)
- Cloud systems
  - Specific information
    - changes of files
    - Dataportability (MS, Google,
    - Export AD data (azure)
  - Define what you collect due to posibility of large amounts of data
    - Takeouts
    - File activity
    - Sharing history
    - Login and trafic information
    - Files deleted / changed
    - Logs of the above
  - Virtual machines
    - If onpremise , collect memory by hibernate VM (VM ware)
- Live collection (Applies to all)
  - Simply copy the files
  - Tools
    - Velociraptor
    - KAPE
    - CYLR
    - Binalyze IREC
    - Volatility
  - Memory dump (if possible - BE CAREFUL)
    - Dumpit
    - Magnet ramdump
    - FTK
    - and many more
  - Netstat -NAOB
  - Image of Harddrive
    - Make sure you have the tools / adapters
    - Caine, Paladin, Kali etc.
    - Make DD / RAW / E01 / AD1
    - Hash and timestamp
    - Store original copy
  - Documentation
    - Describe the files collected
    - HASH / Integrity calculation (SHA256)
    - Describe the course of action
    - Screenshots from system
    - Filetree (screenshot or cleartext ()tree command))
    - Pictures (camera / mobile phone)
  - Encryption
    - LUKS
    - Filevault
    - Bitlocker
    - Boxcryptor
    - Veracrypt
- Ti