FDCA

Some knowledge sharing about DFIR

Lars Blomgaard

Cybersecurity Specialist

I love to share knowledge about IT-security

You can find me at @linkedin leb56751gvgr

CV

Cybersecurity Specialist

- NNIT - Security Specialist
- NC3 - Digital investigations and prevention
- DSV - Senior IT-Security Architect

Spare time

- Tutor on KEA in Governance and DFIR

KEA - Københavns Erhvervs Akademi - Studies

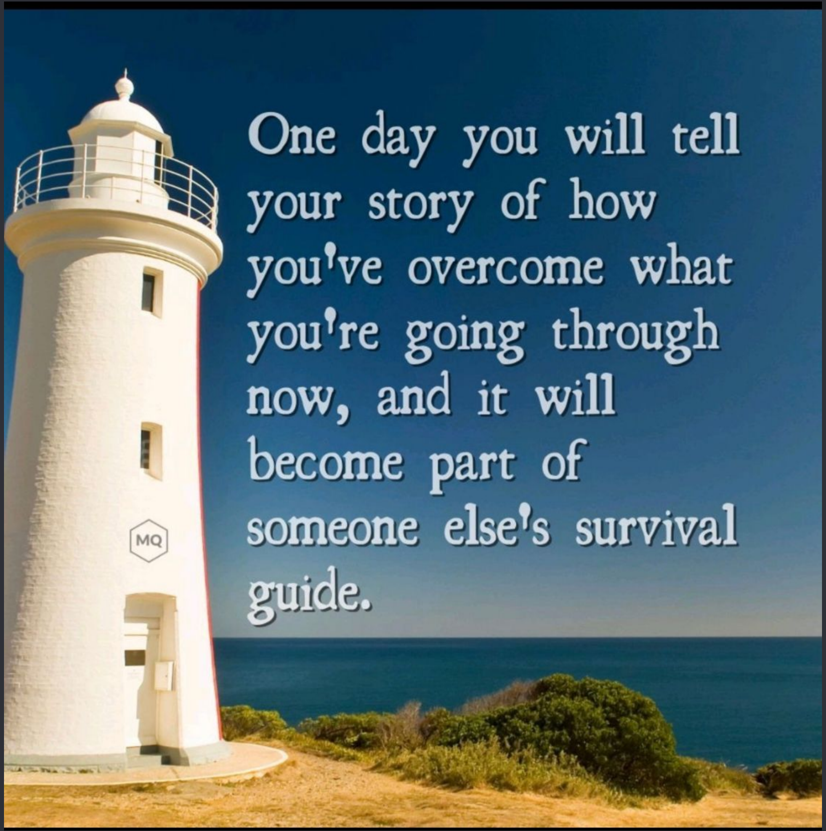
Governance

- ISO, CIS, NIST
- DK Criminal LAW §
- Risk management
- Awareness
- Preparation plans
- Study preparation
- Exam preparation

Threat Handling

- Preparation - technical
- Phases for incident response
- Digital Forensics
- Analysis labs
- File, malware, log, network forensics
- Reporting
- Study preparation
- Exam preparation

My Passion

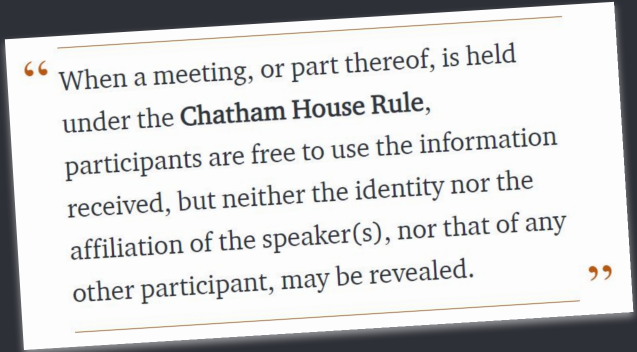

One day you will tell your story of how you've overcome what you're going through now, and it will become part of someone else's survival guide.
MQ

“Disclaimer”

Its my personal experience and knowledge

I do not represent any aforementioned companies.

kea
COPENHAGEN SCHOOL OF DESIGN AND TECHNOLOGY



> “When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.”

Kilde: https://www.chathamhouse.org/chatham-house-rule?gclid=EAIaIQobChMI_vyv4-bL5wIVxOR3Ch3aJAauEAAYASAAEgKR5PD_BwE

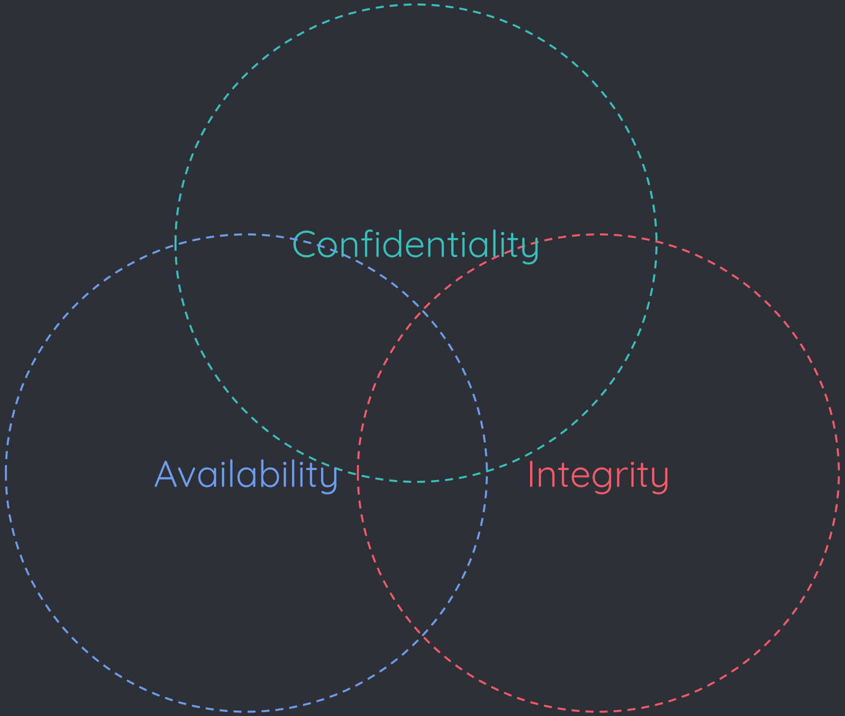
Agenda

- Short look at Governance and the anchor of DFIR
- Threats
- Preparation
- And a discussion based on a case
- Summarize

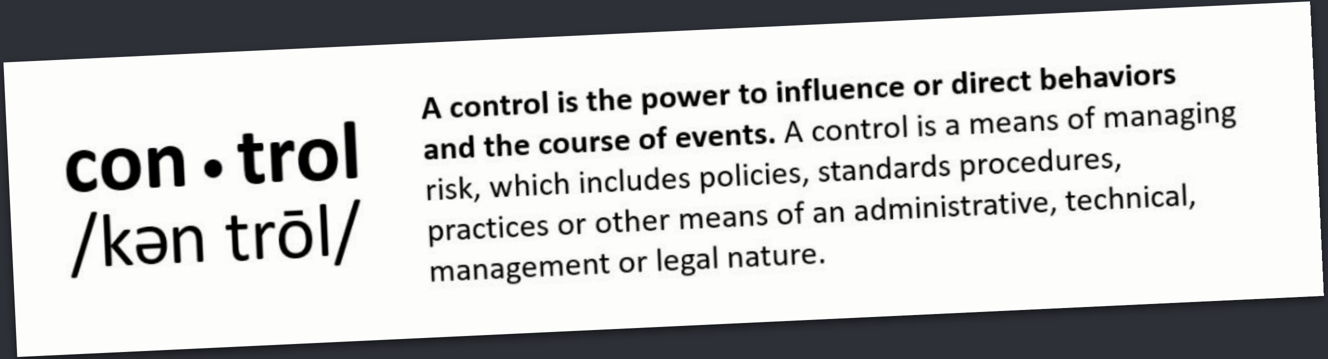
Frameworks

and strategy

CIA



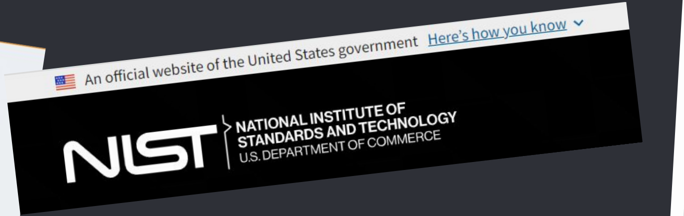
What is a control



con • trol
/kən trōl/

A control is the power to influence or direct behaviors and the course of events. A control is a means of managing risk, which includes policies, standards procedures, practices or other means of an administrative, technical, management or legal nature.

CIS
Center for Internet Security®
Creating Confidence in the Connected World.®


An official website of the United States government
Here's how you know
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

International Organization for Standardization
Organisation internationale de normalisation
ISO

Management

How to we manage information security?

The adversaries make use of

Unpatched systems

People make mistakes, mistakes get into software, software are sold/distributed.

Webpages

Webpages are often overlooked and miss TLC

Embedded systems

Embedded systems, that is on the network gets forgotten. Firmware are software!

Weak passwords

The mother of all fun

Open ports

Services are exposed to the internet. Port 3389 is the gate to doom if left open

No monitoring of service

No monitoring of a service, you don't know the adversaries use bruteforce, no one knows og looks

The adversaries make use of

Forgotten services

If a service is labeled as end of life (EOL). Check it´s EOL. If a vps, this will be abused

Test that went to production

The local IT-hero went to IT-zero, because the system was not backed up

Peoples trust

Phishing, Vishing, Smishing, Social Engineering. We are too trusty against unknown people

People's greed

Employees can turn to malicious actors, if the money is enough

Complexity of a company

Too much technology and compliance will suffocate a business and the overview

The cloud

Can we get transparency in the cloud? Can we se if the systems are used or abused?

What if?

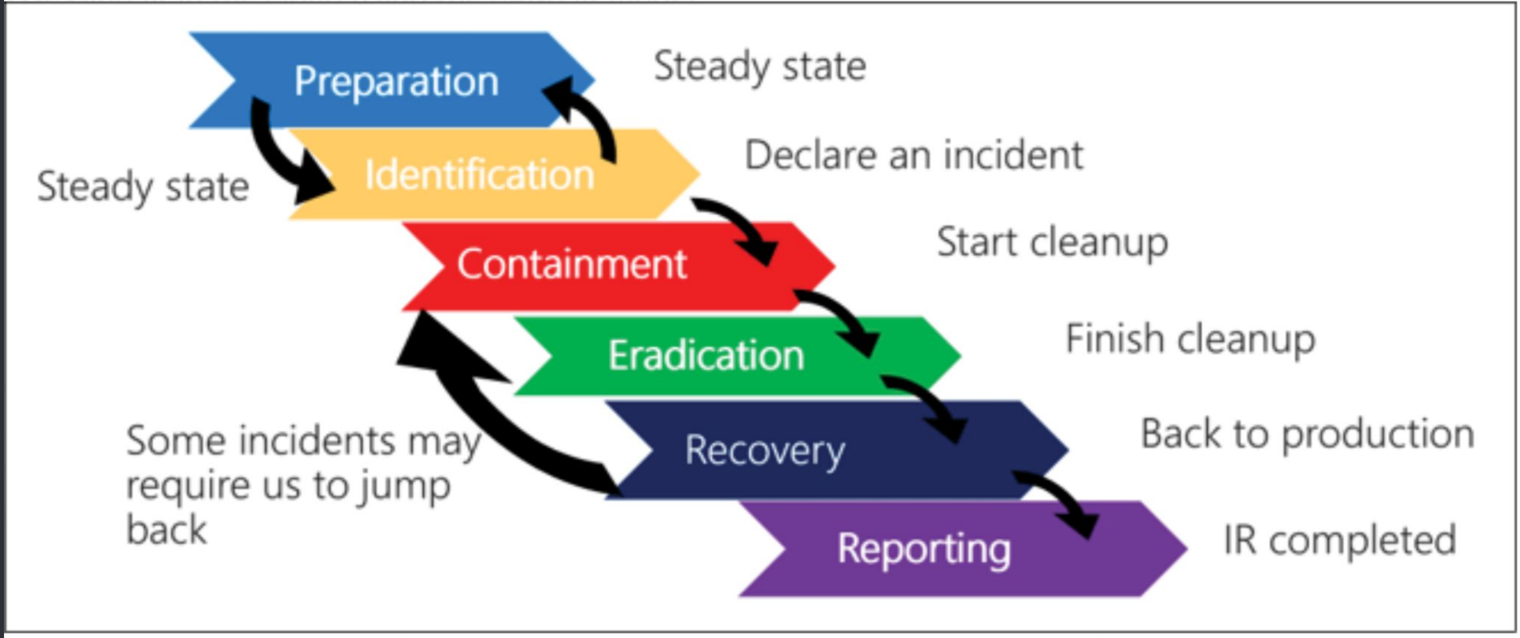
Some of the controls failed

Disaster

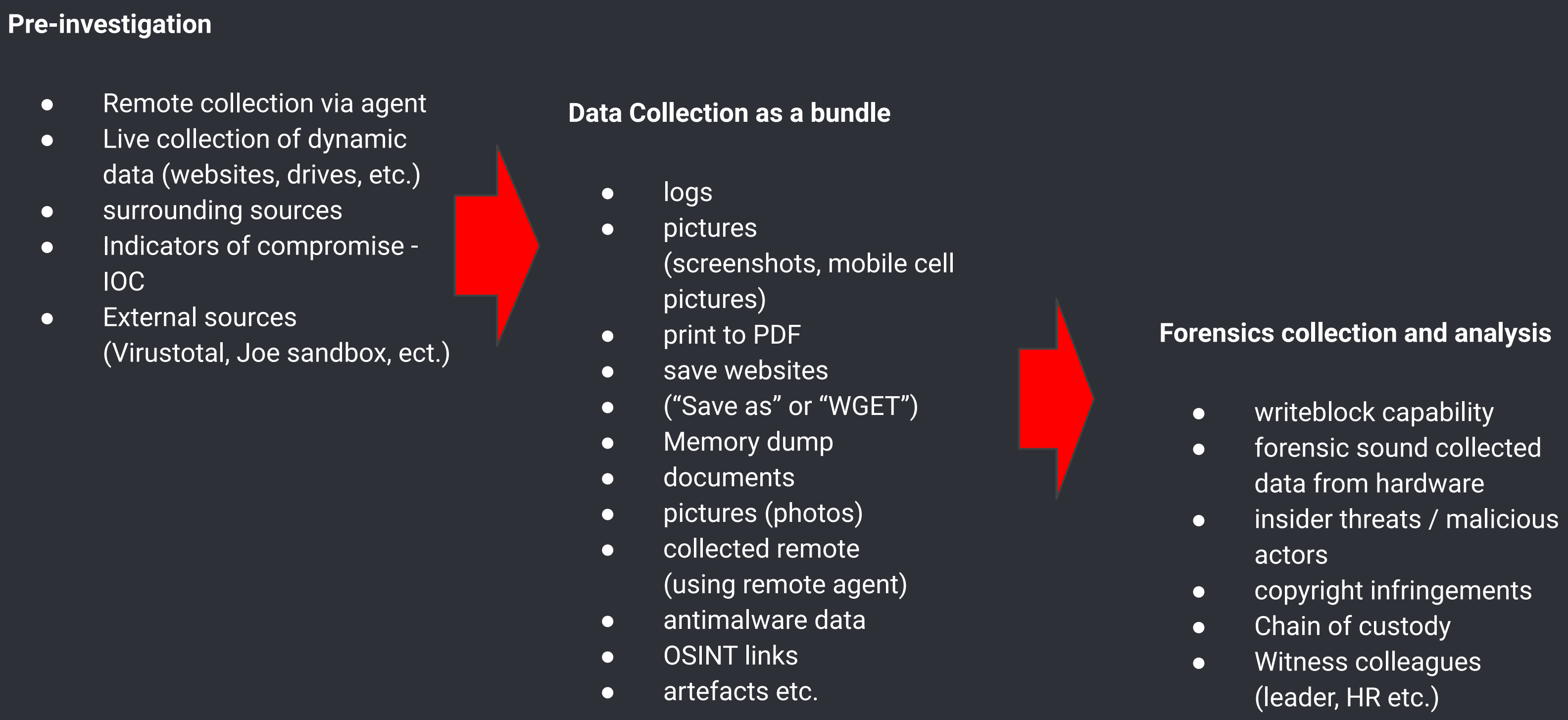
When everything else fails - what then!

Digital Forensics and Incident Response

The better preparation the faster to respond



Decide your capability



Pre-investigation

- Remote collection via agent
- Live collection of dynamic data (websites, drives, etc.)
- surrounding sources
- Indicators of compromise - IOC
- External sources (Virustotal, Joe sandbox, ect.)

Data Collection as a bundle

- logs
- pictures (screenshots, mobile cell pictures)
- print to PDF
- save websites
- (“Save as” or “WGET”)
- Memory dump
- documents
- pictures (photos)
- collected remote (using remote agent)
- antimalware data
- OSINT links
- artefacts etc.

Forensics collection and analysis

- writeblock capability
- forensic sound collected data from hardware
- insider threats / malicious actors
- copyright infringements
- Chain of custody
- Witness colleagues (leader, HR etc.)

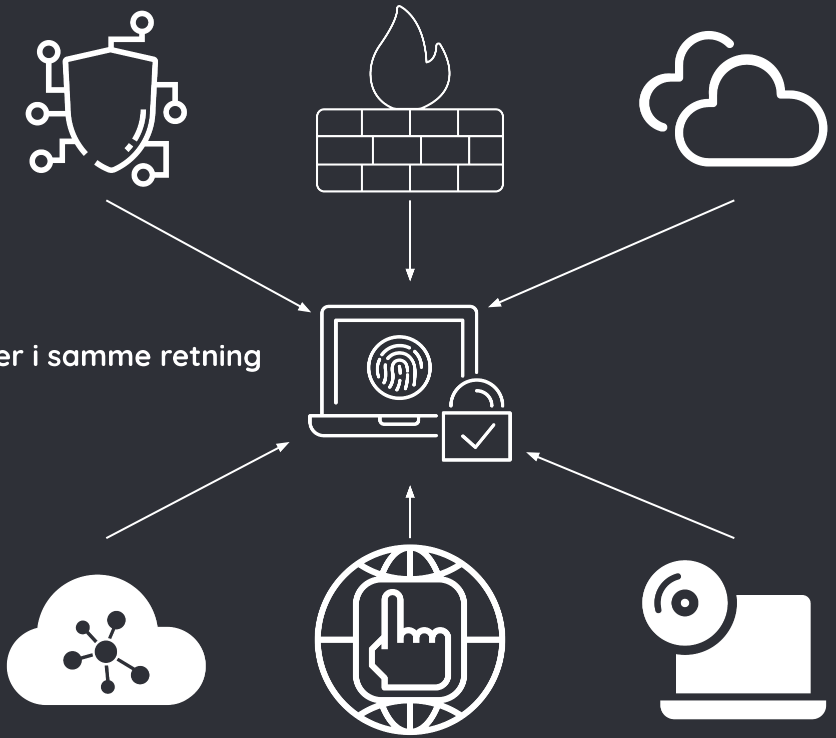
All described as a process

Considerations for evidence?

- Data from more sources that point in the same direction (Triangulation)
- Data must prove the point
  (authenticity)
- Data that comes out of your observations
  (artefacts from systems, malware analysis … Your observables!)
- Data that show what happened and prove the point
  (A Well description of what happened and where its recorded)
- Data have to be admissible
  (Collected using legal methods)

Inspiration: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
And : https://www.nist.gov/forensic-science/interdisciplinary-topics/evidence-management

Det gode bevis - Er det bevis der holder i retten!



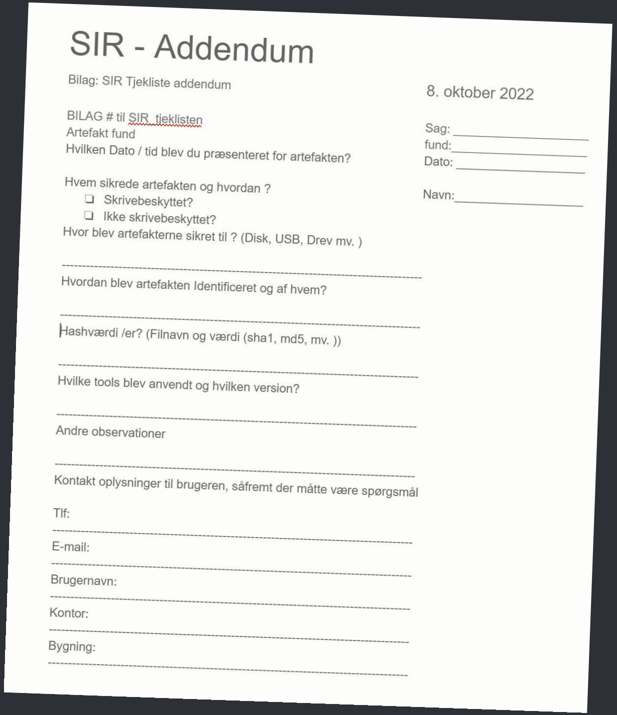
Flere indicier peger i samme retning

Integrity and COC is KEY

- Chain Of Custody
- Sound collection of data. Whether its from hard media, network and Internet.
- Integrity check
- Sound documentation for the process
- Place for secure storage of media, files and data.

Plan your process

- Delegate data responsibility to assigned personnel
- Have addendum for DFIR plan/checklist
  - Where data was collected
  - Who provided the data
  - Time and date
  - With / without writeblocker



SIR - Addendum

Bilag: SIR Tjekliste addendum

8. oktober 2022

BILAG # til SIR tjeklisten
Artefakt fund
Hvilken Dato / tid blev du præsenteret for artefakten?

Sag: ____________
fund: ____________
Dato: ____________

Navn: ____________

Hvem sikrede artefakten og hvordan ?

- ❑ Skrivebeskyttet?
- ❑ Ikke skrivebeskyttet?

Hvor blev artefakterne sikret til ? (Disk, USB, Drev mv.)

Hvordan blev artefakten Identificeret og af hvem?

Hashværdi /er? (Filnavn og værdi (sha1, md5, mv.))

Hvilke tools blev anvendt og hvilken version?

Andre observationer

Kontakt oplysninger til brugeren, såfremt der måtte være spørgsmål

Tlf:

E-mail:

Brugernavn:

Kontor:

Bygning:

KØBENHAVNS ERHVERVSAKADEMI

Plan your process - Remember

What is simple today

Real life is not!

Know your backyard

Case from real world
(Modified for educational purposes)

KEA
KØBENHAVNS ERHVERVSAKADEMI

Case

We are the security team

- A colleague have allegedly done something that looks malicious = violates AUP
- We got the assignment
- Someone mentioned it's gonna be reported to the police!
- This is not a normal operation for the team and we are not prepared

What do we need to do?

What hardware do the company have?

Are you ready to work in the backyard?

- What encryption do we have?
  - How can i get help, in the time of need?
- What hardware is present in our systems?
  - Special needs and do our DFIR hardware work?
- Tools ?
  - Screwdriver, pryers, anti static mats etc.
- Plans that are printed and tested before real life hits
- Do people know what to do?

What Software ?

Do we really have what it takes?

- Are the retainer enough?
- Do we have the software we need, based on past experience ?

Some headaches

Learning as you go

To Disposal

- Mouse and Keyboard
- Corp PC
- Mobile phone

Needs

What we need?

○

○

○

○

My needs

What we need

- Stand Alone PC
- Screwdrivers
- Plekter and plyer
- Software on the PC

To solve this

- Stand Alone PC
- Screwdrivers
- Plekter and plyer
- Software on the PC
  - Arsenal recon
  - FTK
  - Autopsy + ingest modules
- Software on USB
  - Caine and paladin

3 headaches

-
-
-

Pre requisites

3 headaches

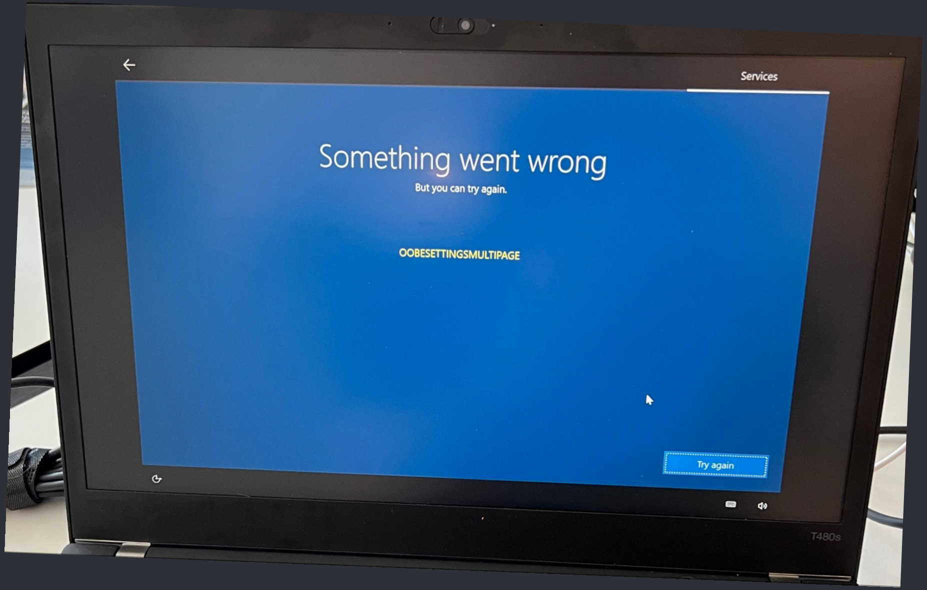
- Access to system (Bios password and bitlocker)
- Read the disk (to do replication)
- Mount the image

I need a supporter with access

Pre requisites

- At the time
  - If all else fails, we need to log on as local admin
    - Needs supporter and access

What Software ?



Services

Something went wrong

But you can try again.

OOBESETTINGSMULTIPAGE

At time of replication

At time of replication

- Curious colleagues
- Relatively new colleague to forensics . We need the learning - knowledge
- No dedicated room / safe storage
- Back up of replication

Mounting data with bitlocker - the solution

- Stand alone machine with
- Arsenal recon image mounter (free verison)
- Autopsy + ingest modules
- KAPE (as a backup and learning)

Arsenal mounted E01

Autopsy looked/mounted the files/drive

Note of caution!

Autopsy is great, but not perfect

Sometimes this crashes, stalls duplicates (after a crash)

Kape

Will generate a lot of data

My lessons

Learned through pain, headaches and hairloss

Lessons learned

- Get your support and expectation align.
- Preparation is key
  - Tools both software hardware
  - Procedures, actions and reporting.
  - Replication capability (hw/sw writeblock and HASHing)
  - Have allies (Support, management, HR, governance team)
- Know your backyard (Hardware, software and quirks and crevasse to you investigations)
- Setup requirements for your tooling
  - Hardware for your PC and the software you need
- Licensed vs open source software. What is enough
- Boundaries between company and retainer agreement.
- Have a forensic room, for carrying out your work
- Require the time needed for the investigative work, based on the alignment.

My suggestions ?

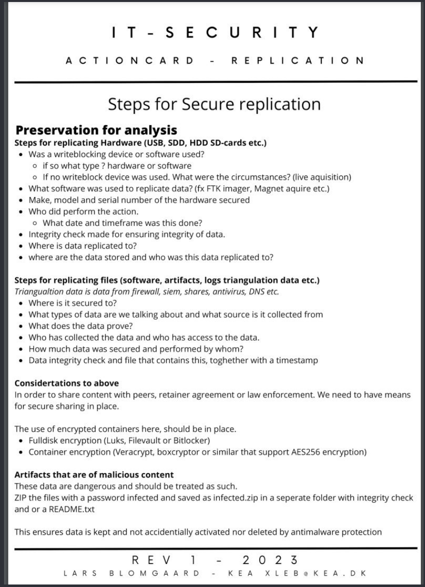
My toolbox

- KAPE
- Arsenal Recon
- FTK imager / magnet imager
- Autopsy or Magnet Axiom
- Loki scanner (Nice 2 have)
- DIRhash
- EZ tools - timeline explorer, hasher, and many more
- Paladin / Caine USB live image
  - And hardware writeblock (know them well)
- Hardware tools - WB,
- Forensic computer
  - 64+ gb RAM, 2 + TB nvme storage, 9 TB HDD storage, i7 /I9 / thread ripper CPU, rtx 3080 +
- Caine 13 PC with SW WB

The better preparation the faster to respond

The better preparation the faster to respond

Have a clear plan and actions



IT-SECURITY

ACTIONCARD - REPLICATION

Steps for Secure replication

Preservation for analysis

Steps for replicating Hardware (USB, SDD, HDD SD-cards etc.)

- Was a writeblocking device or software used?
  - if so what type ? hardware or software
  - If no writeblock device was used. What were the circumstances? (live aquisition)
- What software was used to replicate data? (fx FTK imager, Magnet aquire etc.)
- Make, model and serial number of the hardware secured
- Who did perform the action.
  - What date and timeframe was this done?
- Integrity check made for ensuring integrity of data.
- Where is data replicated to?
- where are the data stored and who was this data replicated to?

Steps for replicating files (software, artifacts, logs triangulation data etc.)

Triangualtion data is data from firewall, siem, shares, antivirus, DNS etc.

- Where is it secured to?
- What types of data are we talking about and what source is it collected from
- What does the data prove?
- Who has collected the data and who has access to the data.
- How much data was secured and performed by whom?
- Data integrity check and file that contains this, toghether with a timestamp

Considertations to above

In order to share content with peers, retainer agreement or law enforcement. We need to have means for secure sharing in place.

The use of encrypted containers here, should be in place.

- Fulldisk encryption (Luks, Filevault or Bitlocker)
- Container encryption (Veracrypt, boxcryptor or similar that support AES256 encryption)

Artifacts that are of malicious content

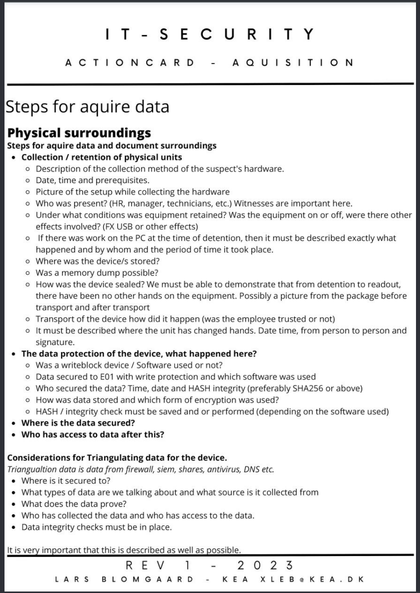
These data are dangerous and should be treated as such.

ZIP the files with a password infected and saved as infected.zip in a seperate folder with integrity check and or a README.txt

This ensures data is kept and not accidentially activated nor deleted by antimalware protection

REV 1 - 2023

LARS BLOMGAARD - KEA XLEB@KEA.DK



IT-SECURITY

ACTIONCARD - AQUISITION

Steps for aquire data

Physical surroundings

Steps for aquire data and document surroundings

- **Collection / retention of physical units**
  - Description of the collection method of the suspect's hardware.
  - Date, time and prerequisites.
  - Picture of the setup while collecting the hardware
  - Who was present? (HR, manager, technicians, etc.) Witnesses are important here.
  - Under what conditions was equipment retained? Was the equipment on or off, were there other effects involved? (FX USB or other effects)
  - If there was work on the PC at the time of detention, then it must be described exactly what happened and by whom and the period of time it took place.
  - Where was the device/s stored?
  - Was a memory dump possible?
  - How was the device sealed? We must be able to demonstrate that from detention to readout, there have been no other hands on the equipment. Possibly a picture from the package before transport and after transport
  - Transport of the device how did it happen (was the employee trusted or not)
  - It must be described where the unit has changed hands. Date time, from person to person and signature.
- **The data protection of the device, what happened here?**
  - Was a writeblock device / Software used or not?
  - Data secured to E01 with write protection and which software was used
  - Who secured the data? Time, date and HASH integrity (preferably SHA256 or above)
  - How was data stored and which form of encryption was used?
  - HASH / integrity check must be saved and or performed (depending on the software used)
- **Where is the data secured?**
- **Who has access to data after this?**

Considerations for Triangulating data for the device.

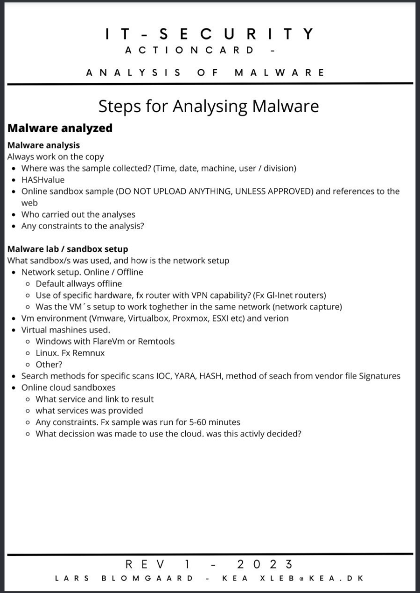
Triangualtion data is data from firewall, siem, shares, antivirus, DNS etc.

- Where is it secured to?
- What types of data are we talking about and what source is it collected from
- What does the data prove?
- Who has collected the data and who has access to the data.
- Data integrity checks must be in place.

It is very important that this is described as well as possible.

REV 1 - 2023

LARS BLOMGAARD - KEA XLEB@KEA.DK



IT-SECURITY
ACTIONCARD -

ANALYSIS OF MALWARE

Steps for Analysing Malware

Malware analyzed

Malware analysis

Always work on the copy

- Where was the sample collected? (Time, date, machine, user / division)
- HASHvalue
- Online sandbox sample (DO NOT UPLOAD ANYTHING, UNLESS APPROVED) and references to the web
- Who carried out the analyses
- Any constraints to the analysis?

Malware lab / sandbox setup

What sandbox/s was used, and how is the network setup

- Network setup. Online / Offline
  - Default allways offline
  - Use of specific hardware, fx router with VPN capability? (Fx Gl-Inet routers)
  - Was the VM´s setup to work toghether in the same network (network capture)
- Vm environment (Vmware, Virtualbox, Proxmox, ESXI etc) and verion
- Virtual mashines used.
  - Windows with FlareVm or Remtools
  - Linux. Fx Remnux
  - Other?
- Search methods for specific scans IOC, YARA, HASH, method of seach from vendor file Signatures
- Online cloud sandboxes
  - What service and link to result
  - what services was provided
  - Any constraints. Fx sample was run for 5-60 minutes
  - What decission was made to use the cloud. was this activly decided?

REV 1 - 2023

LARS BLOMGAARD - KEA XLEB@KEA.DK

Download here: https://www.defencia.dk/dfir/actioncards

Remote collection

And the future

Decide your capability

Pre-investigation

- Remote collection via agent
- Live collection of dynamic data (websites, drives, etc.)
- surrounding sources
- Indicators of compromise - IOC
- External sources (Virustotal, Joe sandbox, ect.)

Data Collection as a bundle

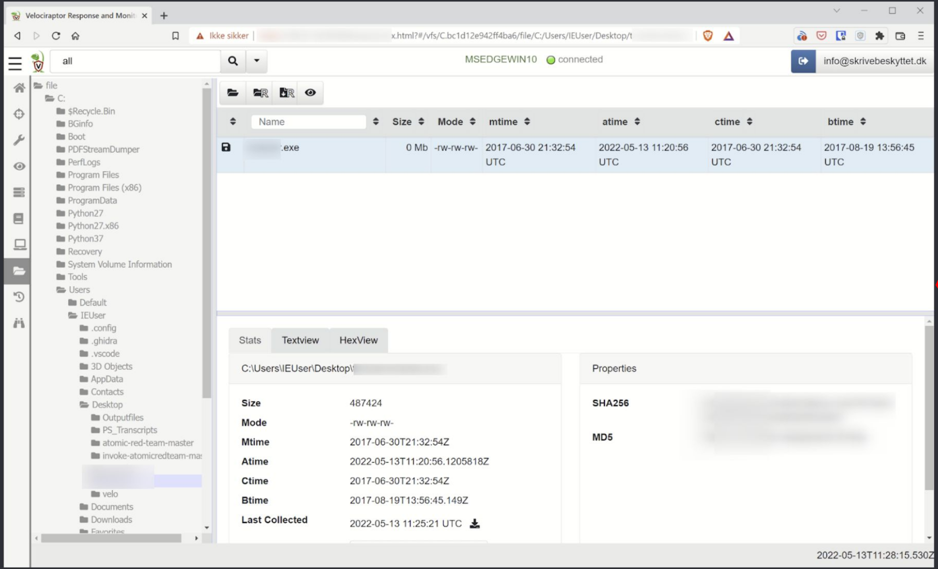
- logs
- pictures (screenshots, mobile cell pictures)
- print to PDF
- save websites
- (“Save as” or “WGET”)
- Memory dump
- documents
- pictures (photos)
- collected remote (using remote agent)
- antimalware data
- OSINT links
- artefacts etc.

All described as a process

Traditional forensics collection

- writeblock capability
- forensic sound collected data from hardware
- insider threats / malicious actors
- copyright infringements
- Chain of custody
- Witness colleagues (leader, HR etc.)

Example - Velociraptor



[redacted]x.html?#/vfs/C.bc1d12e942ff4ba6/file/C:/Users/IEUser/Desktop/t[redacted]

MSEDGEWIN10 ● connected

info@skrivebeskyttet.dk

- file
  - C:
    - $Recycle.Bin
    - BGinfo
    - Boot
    - PDFStreamDumper
    - PerfLogs
    - Program Files
    - Program Files (x86)
    - ProgramData
    - Python27
    - Python27.x86
    - Python37
    - Recovery
    - System Volume Information
    - Tools
    - Users
      - Default
      - IEUser
        - .config
        - .ghidra
        - .vscode
        - 3D Objects
        - AppData
        - Contacts
        - Desktop
          - Outputfiles
          - PS_Transcripts
          - atomic-red-team-master
          - invoke-atomicredteam-mas
          - [redacted]
          - velo
        - Documents
        - Downloads
        - Favorites

	Name	Size	Mode	mtime	atime	ctime	btime
	[redacted].exe	0 Mb	-rw-rw-rw-	2017-06-30 21:32:54 UTC	2022-05-13 11:20:56 UTC	2017-06-30 21:32:54 UTC	2017-08-19 13:56:45 UTC

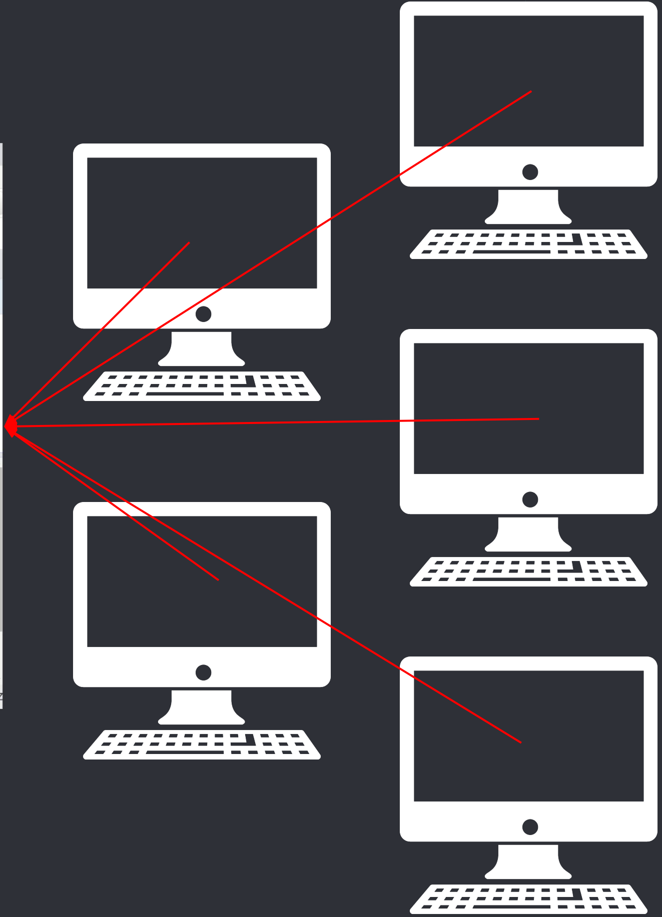
C:\Users\IEUser\Desktop\[redacted]

Size	487424
Mode	-rw-rw-rw-
Mtime	2017-06-30T21:32:54Z
Atime	2022-05-13T11:20:56.1205818Z
Ctime	2017-06-30T21:32:54Z
Btime	2017-08-19T13:56:45.149Z
Last Collected	2022-05-13 11:25:21 UTC

Properties

SHA256	[redacted]
MD5	[redacted]

2022-05-13T11:28:15.530Z



New age - Cloud

Know you backyard

- K8
- VM´s
- Docker
  - What containers do you have?
  - Supply chain for this
  - Pre validation / code check
- Logs at your disposal / visibility?
- Access to data

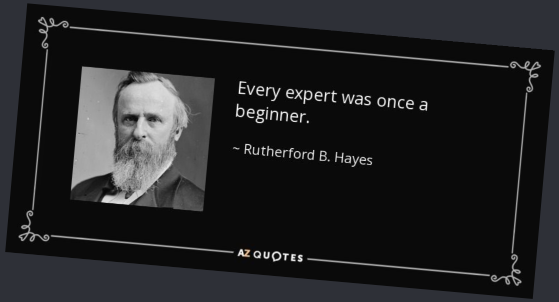
How long time to download / acquire ?

Round up

Summarize

Takeaways

- Know the framework in your company
- Get into the process and understand the key areas
- Build you own space here and argument your choices
- Learn from each other - its a team effort
- Document your actions
- Know how to “sell” your arguments.
- Believe in yourself, you learn as you go



Every expert was once a beginner.

~ Rutherford B. Hayes

AZ QUOTES

Thanks!

ANY QUESTIONS?

Slideshow

https://tinyurl.com/defencia

Kontakt: info@skrivebeskyttet.dk

Web defencia.dk