
Your data Your evidence!

Lars Blomgaard

Cybersecurity Specialist

Passion for sharing knowledge about IT-security -
This i my little contribution - **representing only me!**

Agenda

- Why collect data
- What is good evidence
- Prepare your DFIR plan
- Describe process for collecting
- Integrity of data
- Prepare to share

Caveat

- I am **biased towards my old job**!

  “It’s also **what drives me** to this presentation”
- It’s not a promise, **its lessons learned**, based on my experience
- It’s **up to you to report** or not, im neutral in that sense.

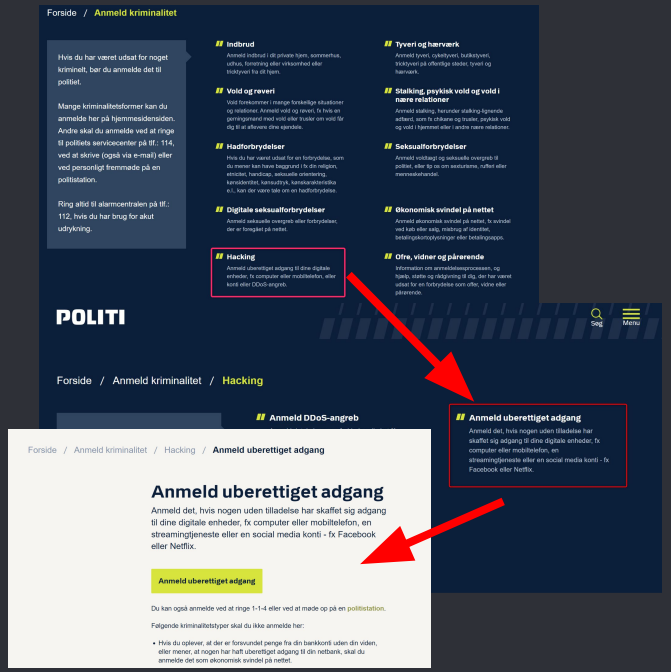
The Problem

The criminals have it too easy!

The issue

- A lot of companies are **being attacked every day**
- It's **way too easy** for the criminals
- Compared to physical world, there is a difference in the amount prosecutions

The Authorities - Ask before you report



Link = https://politi.dk/anmeld-kriminalitet

Why the authorities?

- Give the authorities the power to **investigate and prosecute as they are supposed to do.** Else cybercrime will continue!

- We need to keep **politicians accountable and informed!** To make decisions going forward!

This will increase the **chance of an investigation and prosecution**

Why collect data?

Kære ,

De har 2021 anmeldt afpresning via ransomware til politiet. I den forbindelse har vi brug for de nedenfor oplistede oplysninger for at kunne behandle Deres sag:

- Baggrundsbillede eller tekstfil, som gerningsmanden har lagt på computeren, hvor der angives kontaktoplysninger. Helst original format.
- 3 krypterede filer på max ca. 5 mb. Gerne .zip eller .7Z fil.
- Kopi af filer, programmer eller andet der ved gennemgang af serveren findes efterladt af gerningsmændene. Fx krypteringssoftwaren. Gerne som .zip eller .7Z fil.
- Hvis det konstateres at adgangen til forurettedes computer var gennem RDP (Remote Desktop Port), så hvis muligt en kopi af hele loggen for den kompromitterede RDP port.
- Kopi af spor som gerningsmændene har efterladt i deres forsøg på at fremme deres brugerstatus.

Hvis der eventuelt skulle være andet på computerne/serverne, som I vurderer kunne have interesse for sagen, så et kopi af dette.

- Dokumentation for køb af Bitcoins i form af udvidet betalings- / overførselskvittering.
- Dokumentation for overførsel af de oplyste BTC sammen med dokumentation for afsender og modtageradresser.
- Redegørelse for hvorvidt forurettede eller dennes repræsentant har rettet henvendelse til kryptobørser eller lignende med henblik på indsigelse. I bekræftende fald dokumentation herfor.
- Mailkorrespondance med gerningsmanden (vedhæftet mails fra gerningsmanden fra første mail-modtager, så mailheaderen kan udlæses).
- Dekrypteringsfiler typisk decrypt.exe, som blev benyttet til at låse filerne op.

Det hele må gerne samles i en .zip eller .7Z fil.

Det er politiets anbefaling, at der ikke betales løsesum.

- Der er mulighed for at finde dekrypteringsværktøjer på NoMoreRansom.org, der måske kan dekryptere jeres filer. Alternativt kan harddisken gemmes, da siden opdateres løbende.

Dokumenterne bedes i én sammenfattende e-mail sendt hurtigst muligt og senest inden 14 dage til adressen: KBH-LCIK-sek3@politi.dk -I emnefeltet bedes De skrive journalnummeret: 01 LC-.

Når politiet modtager dokumenterne, vil de blive vedlagt Deres sag. Såfremt De har spørgsmål, bedes De rette henvendelse på e-mail: KBH-LCIK@politi.dk

Såfremt politiet ikke modtager oplysningerne, kan det betyde, at politiet ikke har mulighed for at efterforske sagen.

Side 1

Såfremt politiet ikke modtager oplysningerne, kan det betyde, at politiet ikke har mulighed for at efterforske sagen.

Expectations

When a crime has been committed, the **police begin investigating the case if there are clues or other information that could lead to the case being solved**. Normally, the police start the investigation by questioning the person or persons who know or have seen something relevant to the case.

There may also be **technical clues that the police must investigate**. It can be fingerprints, DNA traces or recordings **from video surveillance**.

If the police believe that there are **reasonable grounds to suspect a particular person, the police will charge him or her with the crime.** When the investigation is over, the prosecutor's office decides what to do next.

Source: https://anklagemyndigheden.dk/da/anmeldelse-og-efterforskning

Police task

The task of the police is to maintain **security, peace and order** - to monitor that the laws are observed and to **take action against offenses by investigation** and **prosecution.** The police also have administrative tasks, such as issuing weapon permits. In addition, the police also have tasks within **total defense in Denmark**.

Source: https://www.forsvaret.dk/da/opgaver/nationale-opgaver/Totalforsvaret/
Source: https://www.justitsministeriet.dk/ministeriet/justitsvaesenet/politi-2/

Evidence

What is good evidence?

“Anonymous”

The best evidence,

is the evidence you´ve got!

This leads to forensics and what is this?

“methods of solving crimes, involving examining the objects or substances that are” involved in the crime

“However, forensics is not just important in the courtroom; forensic evidence needs to be found before any scientific discussion in court can take place. This evidence is found by forensic scientists by performing certain jobs in fields such as chemistry, biology, psychology and even mathematics.”

“Forensic is used to describe the work of scientists who examine evidence in order to help the police solve crimes.”

Source: https://dictionary.cambridge.org/dictionary/english/forensic
Source: https://www.merriam-webster.com/dictionary/forensic
Source: https://www.collinsdictionary.com/dictionary/english/forensic
Source: https://www.crimemuseum.org/crime-library/forensic-investigation/definition-of-forensics/

What is a good piece of evidence?

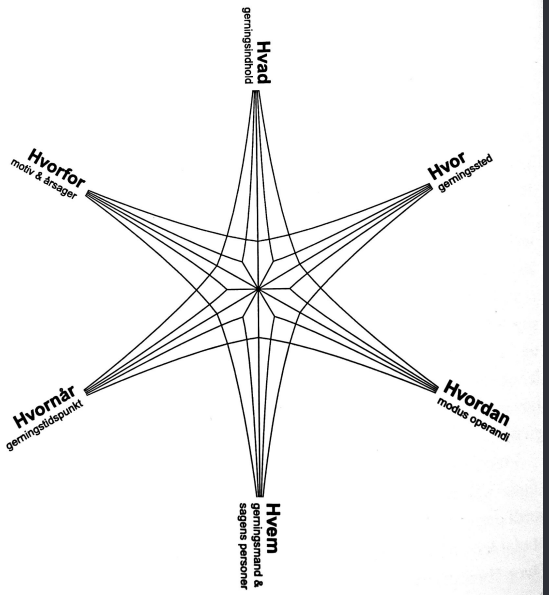
- Data from more sources that point in the same direction
  (Triangulation)
- Data must prove the point
  (authenticity)
- Data that comes out of your observations
  (artefacts from systems, malware analysis … Your observables!)
- Data that show what happened and prove the point
  (A Well description 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

Think like the Police

Investigation star

- What
- Where
- How
- Who
- When
- Why



Figur 3.4. Efterforskningsstjernen.

Source:
https://www.saxo.com/dk/om-at-opdage_karl-ask-adam-diderichsen-ivar-a-fahsing-camilla-hald-vincent-f-hendricks-bjarke-viskum-kira_pdf_9788759322277

Prepare

Your DFIR plan and readyness

Prepare, collect, conquer

- Prepare for **collecting the data**
- Describe your process
- Make it a part of your DFIR plan
- Spending a little extra, goes a long way
- Assign a person to be responsible

Test your tools, know your capability

- Knowing tools and their usage and know its limitations
- Make a process for data collection across the business
- Do you have the necessary setup for analysis? (Hardware, network, software etc.)

Examples of escalation/collection

Escalation chart - severity escalation

Escalation Chart with Examples (This table is not inexhaustible)

severity	event	action	Capacity	Report to authorities	Preparation
level 1 (Low)	• potentially unwanted programs (PUP) • warning banners • clean alerts from antimalware solution • Adware	• Delete the files • Remove the software / service	• Normal operations • Register the event	no	• Normal service and follow up of Antimalware services.
level 2 (mid)	• Phishing • malware detected and deleted • Macro viruses	• Delete the files • Remove the software / service • Maybe look for online information.	• As level 1 • Escalate if more occurrences are detected	• As information only. Report, don't expect any investigation	• Normal service and follow up of Antimalware services. • validated and tested, response plan
level 3 (High severity and low spread)	• Copyright infringement • malware partially detected • Passwords leaks with e-mail • Spear phishing and data not delivered • Attempts to escalate privileges • Attempts of lateral movement • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Analyze the event to see what is the intention. • Set up monitoring for the events • Prepare for further events and inform management • Monitor closely for activity	• As level 2 • • Collection of data with integrity and timestamps (maybe Forensic less sound) • Carefully describe your process of evidence collection.	• Yes, share data and the identification findings. • Get case/report ID. • Get contact at the police and get JNR number (IT-engineer at NSK/NC3)	• The above, including below • Have updated and tested Incident Response plan • Forensic capability, and les forensic ways of data collection
level 4 (Critical, high impact - high spread - business critical)	• Zero days • APT • Malware not detected and activated • Spear phishing and data delivered • Services have been breached • Accounts have been escalated • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Create a communication plan if needed. (specially of company deliveries to the community) • Analyze the events for the intention. • Prepare 3'rd party	• As level 4 • Designate responsibility to file responsable. • Report to authorities (Get contact to appropriate level (NSK/NC3)) • Physical collect data from media if possible	• Yes, share data and the identification findings. • Get case/report ID • Get contact at the police and get JNR number (IT-engineer at NSK/NC3) • Prepare court case (if needed and	• Major incident plan. • Secondary communications channels

Examples of escalation/collection

A1 | fx | Escalation Chart

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Escalation Chart														
2	Event	Action	Capacity	Preparation capability	Man lab	auto lab	Not WB	WB	Remote analysis	Isolation	Integrity calc	Report to authorities	Inform authorities	Sample Isolation	Severity
3	potentially unwanted programs (PUP)	remove program	monitor for recurrence	Corporate image					x		x				1
4	warning banners	remove program	monitor for recurrence	Corporate image					x		x				3
5	clean alerts from antimalware solution	remove program	monitor for recurrence	Corporate image					x		x				3
6	Adware	remove program	monitor for recurrence	Corporate image					x		x				4
7	Phishing	Rely on Spamfiltering	monitor for recurrence	Corporate image					x		x				5
8	Spear Phishing	analyse threat	analyze with detached system	Lab			x		x		x	x	x	x	8
9	malware detected and deleted	re-install system	monitor for recurrence	Corporate image		x			x	x	x				2
10	malware partially detected	re-stablish system from backup	monitor for recurrence	Corporate image		x			x	x	x				7
11	malwarebehaviour and not detected	re-install system	monitor for recurrence	Corporate image	x	x			x	x	x			x	10
12	Macro viruses	re-install system	monitor for recurrence	Corporate image					x		x			x	8
13	Copyright infringement	Withhold HW ans secure user traces	physical secure evidence	Writeblocker	x		x		x		x			x	10
14	Passwords leaks with e-mail	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				5
15	Spear phishing and data not delivered	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				4
16	Attempts to escalate privileges	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	9
17	Attempts of lateral movement	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	10
18	Usage of CVE 7+ vulnerabilities	re-stablish system from backup	inform senior management of risk	Corporate image + patch			x		x		x			x	9
19	CVE 7+ vulnerabilities identified	Create Risk analysis	governance plan	Forensic analysis and monitor	x		x		x		x				6
20	Rootkits detected on system	Determine MO and escalate to IR	datacollect and re-install	Forensic analysis and monitor	x		x		x		x	x	x	x	9
21	Remote Access Trojan (RAT)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x	x	x	x	10
22	Zero days (internal systems/network)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
23	Zero days (Facing Internet)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x				10
24	APT	Determine MO and calculate risk	restore from backup	Forensic analysis and monitor	x		x		x		x	x	x	x	10
25	unpached systems	Roll into patch mangement	governance plan	Monitor activity			x		x		x				5
26	Malware not detected and activated	Determine action and severity	DFIR plan	Forensic analysis and monitor			x		x		x			x	10
27	Spear phishing and data delivered detected	Determine MO and calculate risk	inform senior management of risk	Monitor activity	x	x	x	x	x	x	x	x	x	x	10
28	Services have been breached	Analyze logs and periphials - restore	DFIR plan	Corporate image			x		x	x	x			x	10
29	Accounts have been escalated	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor			x		x	x	x	x	x	x	8
30	Targeted attacks (unsuccessful)	Determine MO and calculate risk	inform senior management of risk	Forensic analysis and monitor	x	x	x		x		x			x	7
31	Targeted attacks (successful)	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x	x	x		x	x	x	x	x	x	10
32	Insider threats or paid actors	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x	x	x		x	x	x	x	10
33	EOL software (Internal)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
34	EOL software (external)	Determine MO and calculate risk	inform senior management of risk	vulnerability scanner			x		x		x				8
35	EOL hardware	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				4
36	Legacy systems	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
37	User violated AUP	Determine MO and escalate accordingly	warn and inform (monitor)	Plan from HR	x	x	x	x	x	x	x	x	x	x	7
38	User violated AUP intentional	Determine MO and escalate accordingly	datacollect	Plan from HR	x	x	x	x	x	x	x	x	x	x	10

Prepare

your tools and know your capabilities

Special tools

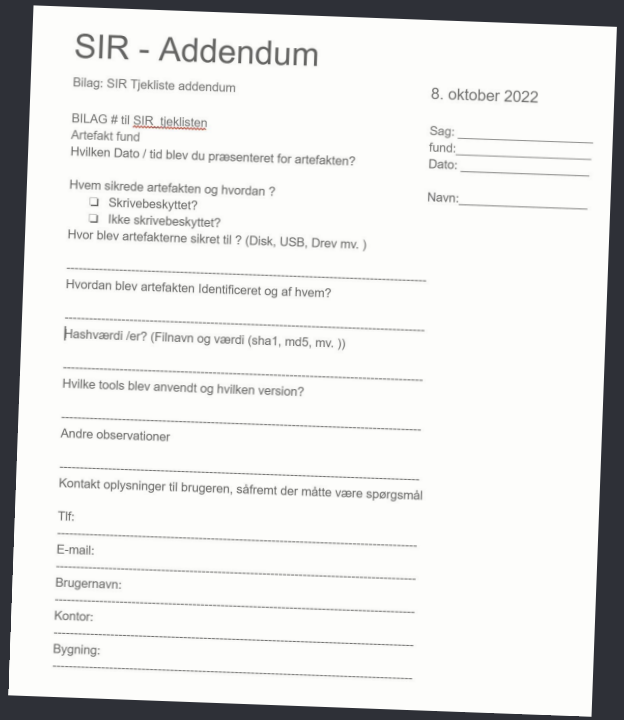
- Writeblock capability
- Data collection to **one place**!
  (and of course backup the data)
- Forensic software

Collect

Process for good collection

Plan your process

- Delegate data responsibility to assigned personel
- 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:

Forensic capability

- Writeblock capability
  (HW or SW)
- Know your environment of hardware
  (IDE, SATA, M.2, PCI-E, USB, SD etc.)
- If needed describe your “chain of custody”
  (Have a safe physical storage or monitored room)

Forensic data collection

- Know your environment for datasources
  - Cloud, NAS, server, endpoint, network etc.
  - Website

    (in case of copyright)
- Have tools at your aid

  (Forensic tools like Magnet Cyber, FTK, Autopsy, cybertriage etc)
- Fx Memory Dump capability

  (Magnet ramdump, dumpit, FTK, Ram Capture etc.)
- Identify your data, your artefact smoking gun

Decide your capability

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.)

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

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.)

Decide your capability

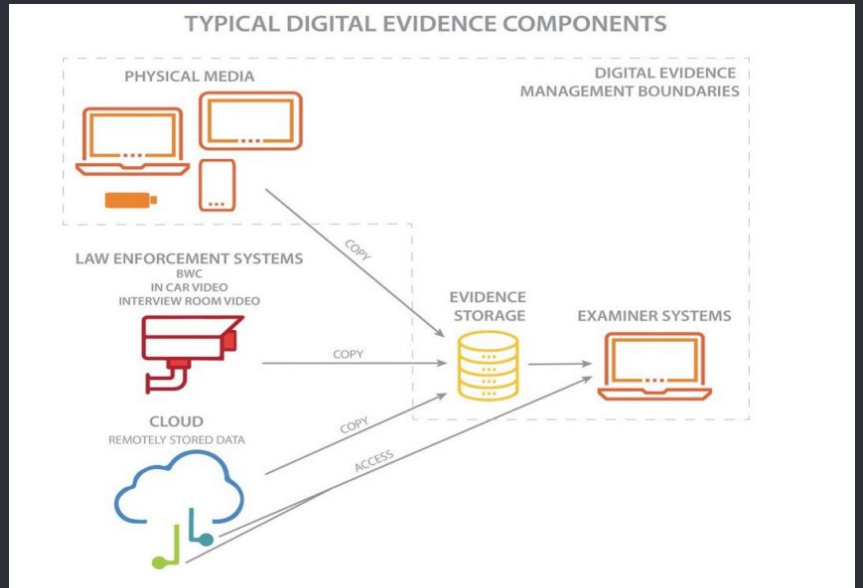


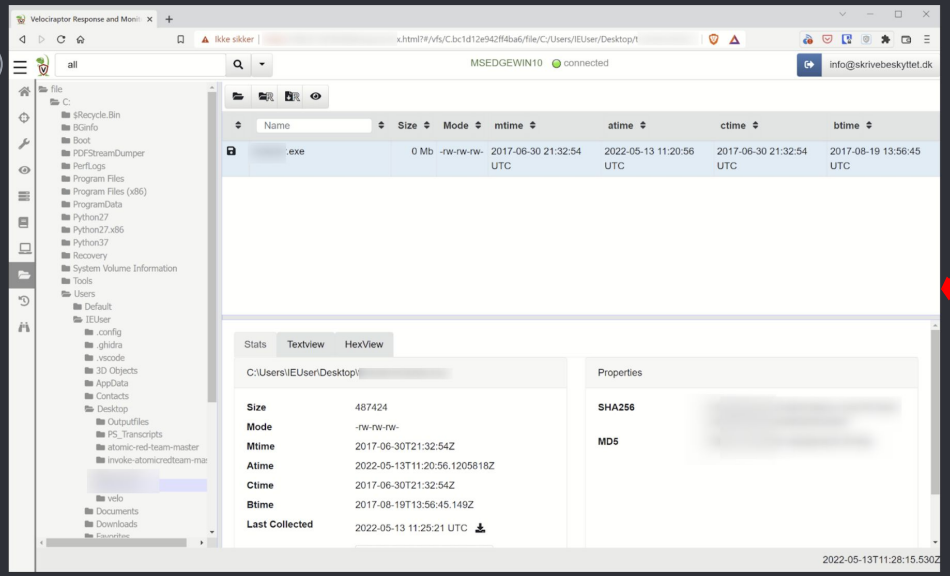
Figure 1. Typical Digital Evidence Components.

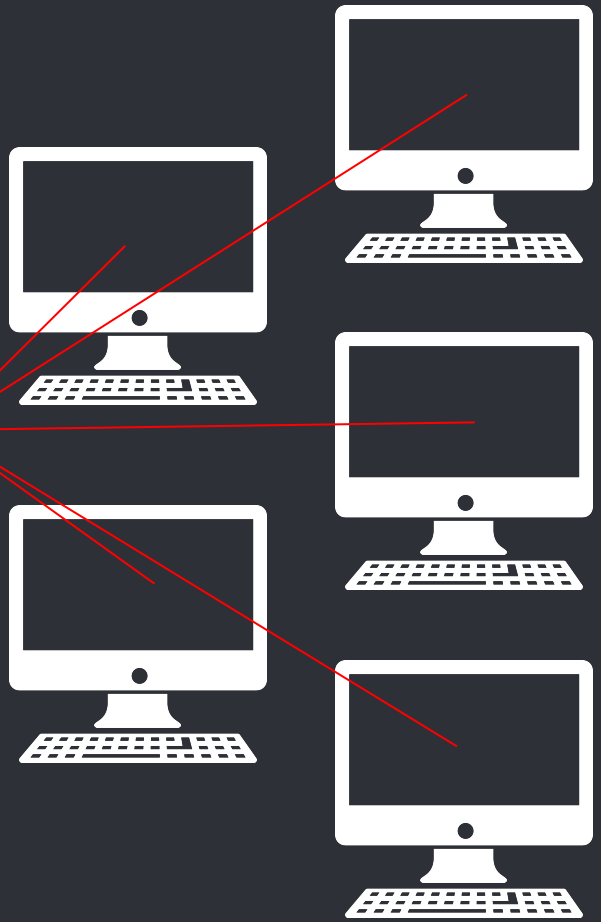
Source: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
And: https://www.nist.gov/forensic-science/interdisciplinary-topics/evidence-management

Remote collect

It's not easy from afar

Example - Velociraptor





Integrity

Freeze time

Integrity is your file DNA

- Use good HASH like SHA256 to avoid hash collision
- Timestamps from the “snapshot”
- Describe the prerequisites of the collection
- Containerize the data, and turn on writeblock
- Make it easy to understand the data and describe it

Example of secure integrity

- Case-24052022-Incident_unwelcome_guests
  - Machine-PC23455_user_arne@virk.dk
  - Machine-PC27255_user_lise@virk.dk
  - Machine-PC45455_user_vibs@virk.dk
  - Server-SV-App234-DK-webserver

Machine-PC23455_user_arne@virk.dk

Navn	Ændringsdato	Type	Størrelse
File1.pptx	23-05-2022 20:27	Microsoft PowerPo...	0 KB
File2.pub	23-05-2022 20:27	Microsoft Publishe...	59 KB
File3.pub	23-05-2022 20:26	Microsoft Publishe...	59 KB
File4.docx	23-05-2022 20:26	Microsoft Word-d...	0 KB
File5.docx	23-05-2022 20:26	Microsoft Word-d...	0 KB
File6.rtf	23-05-2022 20:26	RTF-format	1 KB
File7.xlsx	23-05-2022 20:28	Microsoft Excel-re...	7 KB
HASH_Machine-PC23455_user_arne@	5-2022 20:24	Tekstdokument	1 KB

```
121CF9D2076962FD7D84A67129421915E626E59FB9D2EC8F89E35C7441553E6A  App\AppInfo\File1
573CED9FB3B5DBD183EF144532F3D36CB7D7EF444DC563B7243298DB2359E2DB  App\AppInfo\File2
F17B6E607BFB06E03551AEECE1BC928C0A9E80A42AD12CBE84FC5220145F6225  App\AppInfo\File3
C2048C3343F7837E43887D7AADE05411C165E796DFB82B0CF42438D50810FAE2  App\AppInfo\File4
AE0EEF67EDF75DD9C15E0C2B5653C8628AD42DED2BA0495F9A68E55E439AAD42  App\AppInfo\File5
2C101D62FFE213264CD69DA2118BC1735F2002BAD19C701937E046785BA71570  App\AppInfo\File6
1EBED2D9CD92376A0A27EEBC8C6C54C371DDDDB9F92E7FFFAE878EFCDC8B6059  App\AppInfo\File7
```

- Machine-PC23455_user_arne@virk.dk
- Machine-PC27255_user_lise@virk.dk
- Machine-PC45455_user_vibs@virk.dk
- Server-SV-App234-DK-webserver
- Machine-PC23455_user_arne@virk.dk_2361561673F42360C0431033D379D57C800E64FBB83465D042F764003C165356.zip


Prepare
To share

Do we need to share?

- Reporting to authorities (datatilsynet or police)
- Do we have cloud sharing capability
  - Encryption
  - End share date
  - Password for data
  - One time download (fx boxcryptor)
- **Remember it's your vulnerable moments**

Learn

From your data

Internal awareness

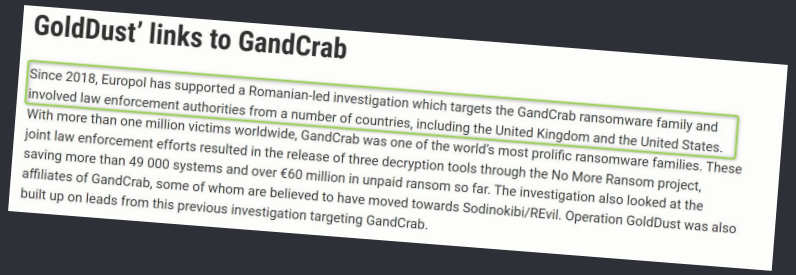
- Can we use the material for training new personal?
- Can we use the data to create awareness for C-level and users in the business?
- We got a “free pentest” use it to your advantage ;)
- Adjust your readiness

Expectations

To the authorities - an allignment

Example of expectation - gandcrab ransomware (approx 3 years)

Europol facilitated the information exchange, supported the coordination of operation GoldDust and provided operational analytical support, as well as cryptocurrency, malware and forensic analysis. During the action days, Europol deployed experts to each location and activated a Virtual Command Post to coordinate the activities on the ground. The international cooperation enabled Europol to streamline victim mitigation efforts with other EU countries. These activities prevented private companies from falling victim to Sodinokibi/REvil ransomware.



GoldDust' links to GandCrab

Since 2018, Europol has supported a Romanian-led investigation which targets the GandCrab ransomware family and involved law enforcement authorities from a number of countries, including the United Kingdom and the United States. With more than one million victims worldwide, GandCrab was one of the world's most prolific ransomware families. These joint law enforcement efforts resulted in the release of three decryption tools through the No More Ransom project, saving more than 49 000 systems and over €60 million in unpaid ransom so far. The investigation also looked at the affiliates of GandCrab, some of whom are believed to have moved towards Sodinokibi/REvil. Operation GoldDust was also built up on leads from this previous investigation targeting GandCrab.

Source: https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

Example of expectation - Antwerp attack (about 2 years)

The hacking took place over a two-year period to June 2013 but appears to have come to an end after police arrested 15 people and seized computer equipment, drugs, firearms — including a machine gun — and a substantial amount of cash in raids in Belgium and the Netherlands.

Vanishing containers

The attack on the port of Antwerp is thought to have taken place over a two-year period from June 2011.

Prosecutors say a Dutch-based trafficking group hid cocaine and heroin among legitimate cargoes, including timber and bananas shipped in containers from South America.

Source: https://www.tradewindsnews.com/weekly/how-hackers-attacked-the-port-of-antwerp/1-1-342065 (paywall)
Source : https://www.bbc.com/news/world-europe-24539417

Example of expectation - Silk road missing BTC (about 10 years)

"For almost ten years, the whereabouts of this massive chunk of missing Bitcoin had ballooned into an over $3.3 billion mystery," commented U.S. Attorney Damian Williams.

"Thanks to state-of-the-art cryptocurrency tracing and good old-fashioned police work, law enforcement located and recovered this impressive cache of crime proceeds."

Source:
https://www.bleepingcomputer.com/news/security/us-unmasks-hacker-who-stole-50-000-bitcoins-from-silk-road/?utm_source=pocket_saves

Example of expectation - sexual child exploitation case (over 2 years)

RETTEN I RANDERS

D O M

afsagt den 27. november 2017

Rettens nr. 5-600/2017
Politiets nr. 4200-72386-00004-15

Anklagemyndigheden
mod
[redacted] Tiltalte
Født den [redacted] Dato 1 1960

Der har medvirket domsmænd ved behandlingen af denne sag.

Anklageskrift er modtaget den 17. februar 2017.

[redacted] Tiltalte er tiltalt for overtrædelse af

straffelovens § 235, stk. 1 og 2, udbredelse og besiddelse af børneporno-
grafi, ved den 24. september 2015 ca. kl. 8.45 på [redacted] Adresse 1
[redacted], Randers C, at have været i besiddelse af 3.091 pornografiske billeder og 2.643 pornografiske filmsekvenser med personer under 18 år, ligesom han i perioden fra den 14. december 2012 til den 23. september 2015 på internettet via fildelingsprogrammet "eMule" distribuerede i alt 9 pornografiske billeder og 3.492 pornografiske filmsekvenser med personer under 18 år.

Source: https://domsdatabasen.dk/webapi/api/Case/document/download/content/1126

Example of expectation - Extorsion (over 3 years)

Københavns Byret

KØBENHAVNS BYRET
DANMARKS DOMSTOLE

Udskrift af dombogen

D O M

afsagt den 9. maj 2016 i sag

SS 1-31954/2015
Anklagemyndigheden
mod
T
Født september 1990

Sagens baggrund og parternes påstande

Denne sag er behandlet som tilståelsessag.

Retsmødebegæring er modtaget den 8. december 2015.

T er tiltalt for

1.

afpresning efter straffelovens § 281, nr. 1,
ved den 27. november 2014 kl. 00.16 for derigennem at skaffe sig uberetti-
get vinding, pr. e-mail at have truet F1 ,
, med at offentliggøre privatlivet tilhørende oplysninger i form af
navne, cpr-numre og journaloplysninger på personer, der havde været i be-
handling i F1 , som behandler børn og unge med seksuelt grænse-
overskridende adfærd og ofre herfor, hvis ikke F1 overførte pen-
ge i form af 2 x 1.500 kr. i Bitcoin til ham.

Source:
https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/85a1e29e-7b81-4a5d-b0aa-0373050353c0?showExact=true

Summarize

A few notes at the end

Summarize - environment

1. Know you environment of log / data sources
2. Know the capability of the above
3. Know your analysis capability
4. Know your plan and tools for the job
5. Know your process for collecting
6. Know your actions (reporting to authorities, vendors, peers etc)
7. Test all of the above

Summarize - process

- Describe the task and tool
- Describe the timeframe
- Describe what you did
  - Maybe record what your did (screenshot / screencast)

The ultimate test to this, is court. **All cases are different**. **Do your best and succeed!**

The Master Goal

Better evidence, for a chance of **investigation** and bringing the **perpetrators to justice!**

Questions

Download presentation here : https://www.defencia.dk/infosec-og-diverse/bsides-2022

Thanks!
Happy huntin´