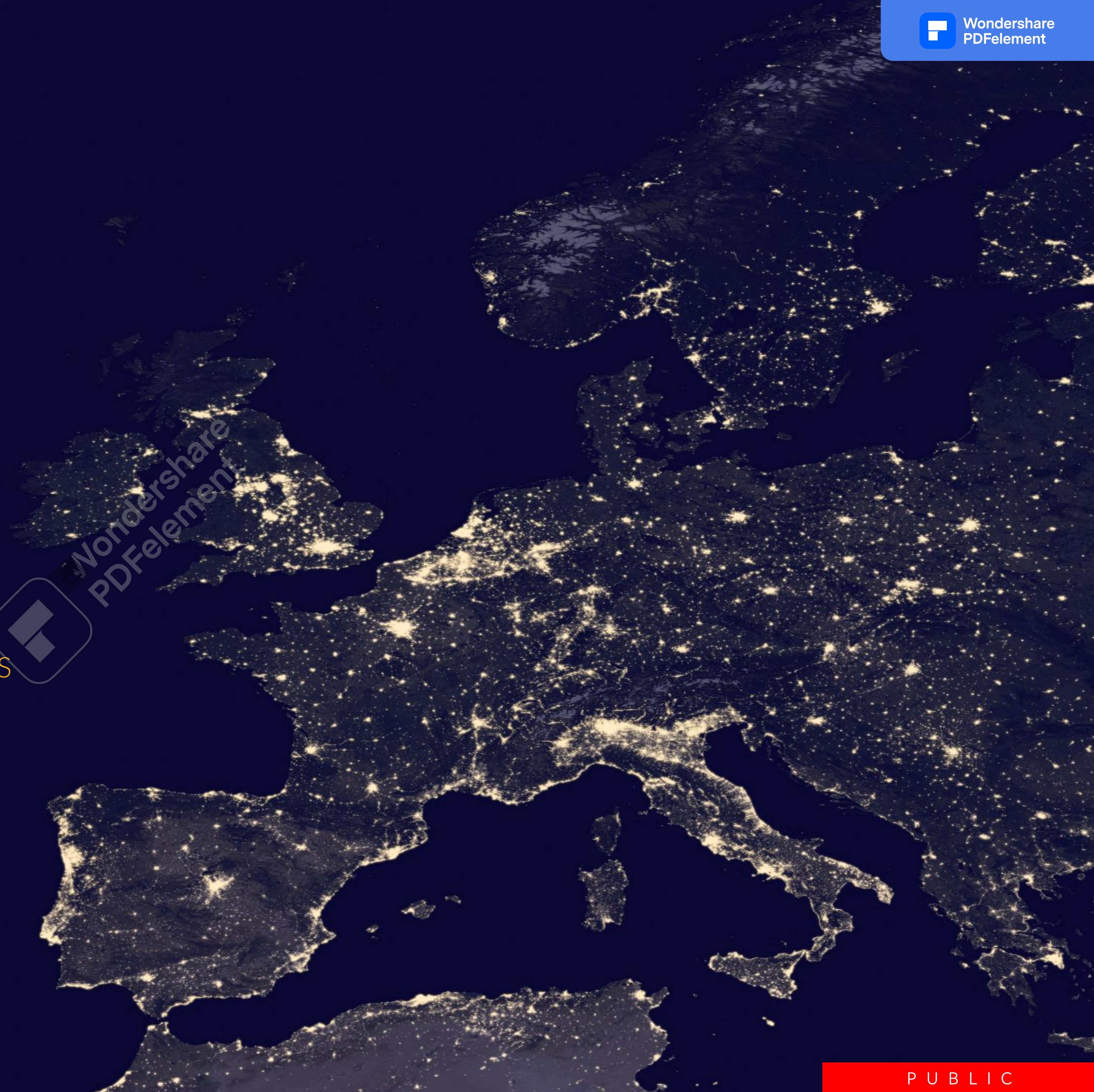
Wondershare
PDFelement

HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES



Wondershare
PDFelement

PUBLIC

Wondershare PDFelement

Automating Incident Response by default

https://www.cbr.com/flintstones-jetsons-same-time-period-theory/

Wondershare PDFelement

Francisco

Zawadi

Wondershare PDFelement

PUBLIC

Wondershare
PDFelement

Our time together

INTERRUPTIONS ALLOWED

IR process

IR Lab

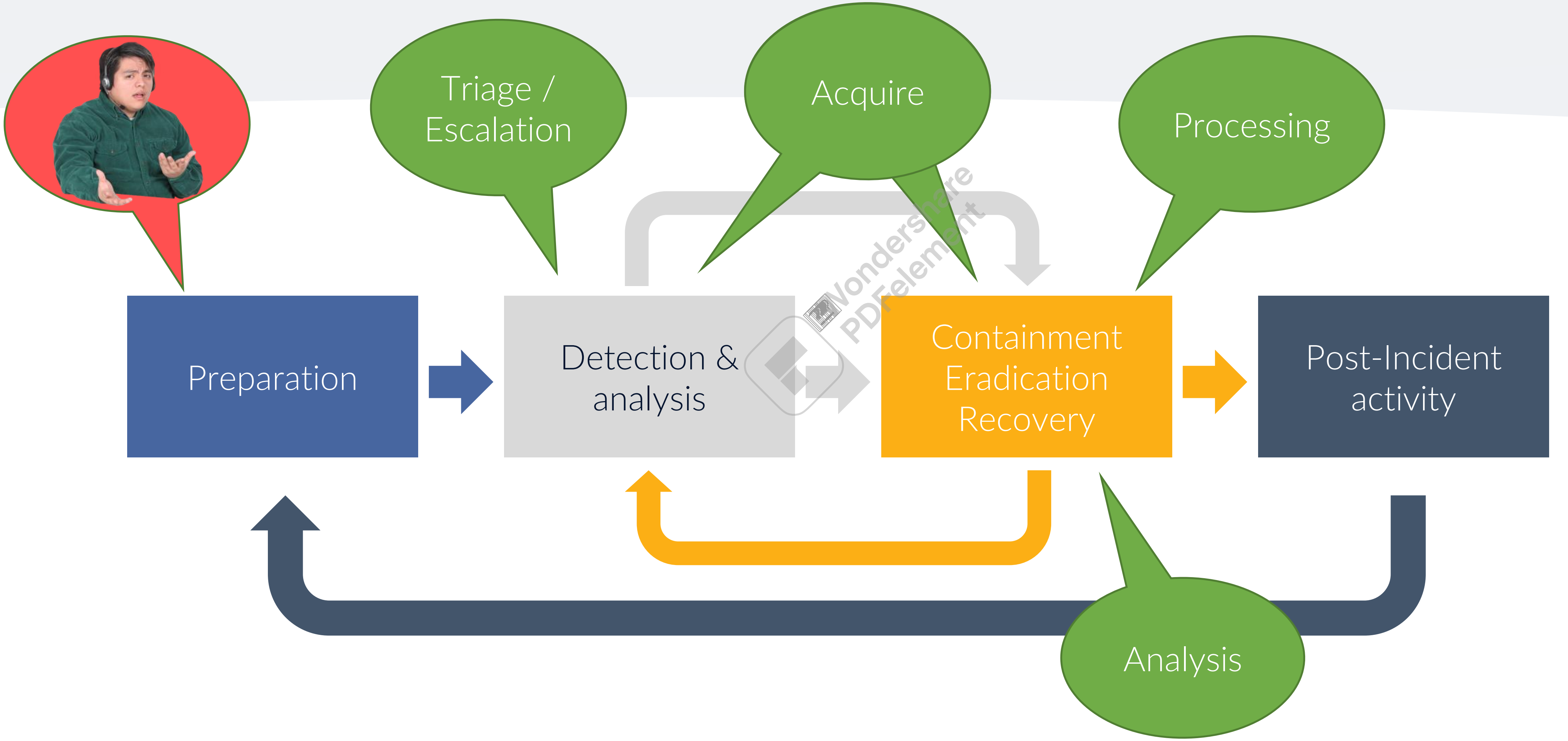
DevOps mindset

Questions

Wondershare
PDFelement

Wondershare PDFelement

Big picture



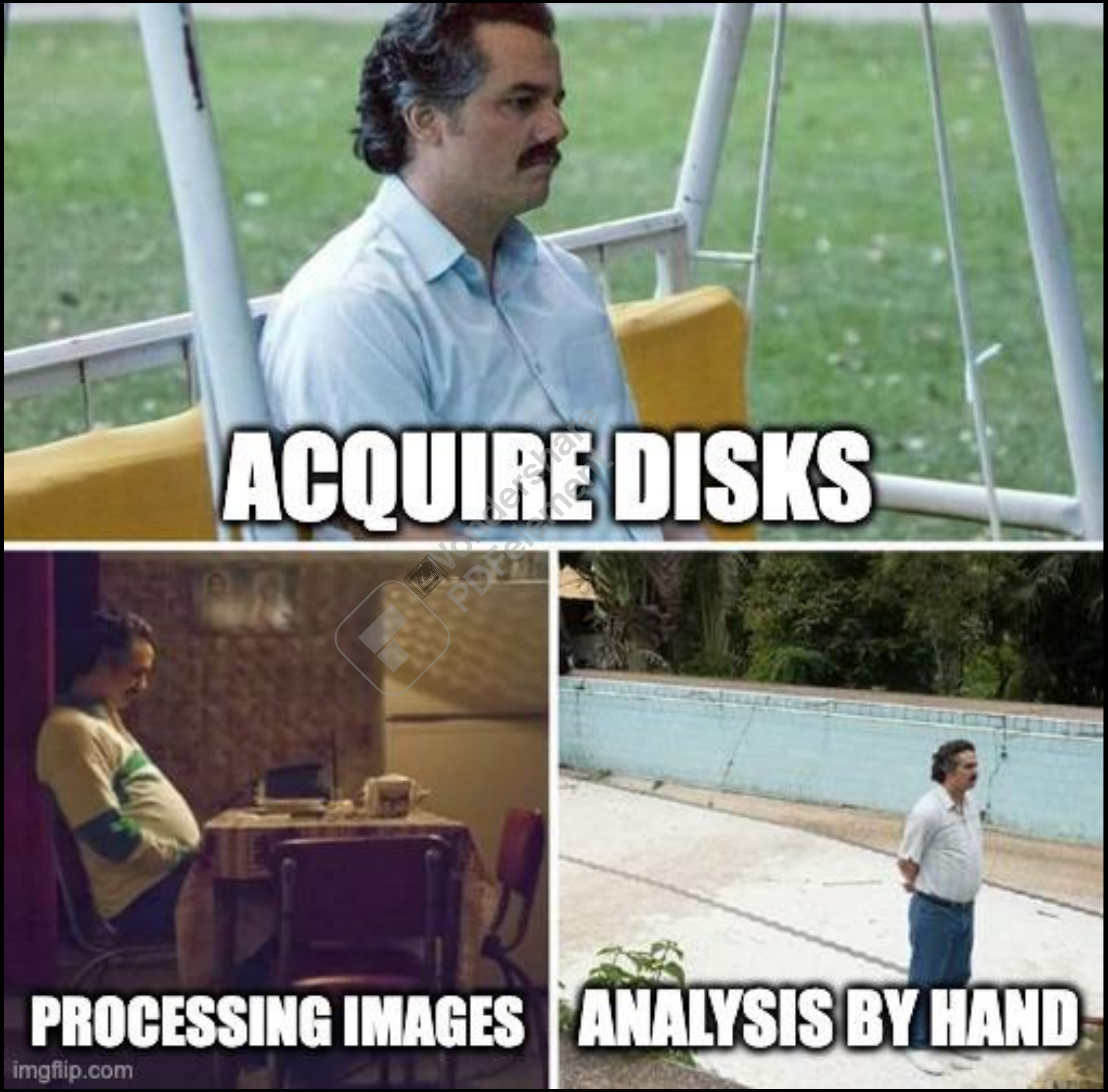
Wondershare PDFelement

Wondershare PDFelement

Big Picture

Wondershare PDFelement

Wondershare
PDFelement



Wondershare
PDFelement

Photo by Daniel Tausis on Unsplash

Acquire

https://www.lifars.com/2021/05/how-to-acquire-digital-evidence-for-forensic-investigation/

Wondershare PDFelement

Wondershare PDFelement

Acquire

CURRENT STATE

- Not scalable manual collection
- Memory is still a weird ‘thing’ to acquire
- Disks of 1TB+ are the new normal
- Duration of acquisition delays processing
- Chain of evidence mostly for audit purposes

Wondershare PDFelement

Wondershare PDFelement

Acquire

DESIRED STATE

- Scalable acquisition across all targets
  - Forensics packages based on data where most likely forensics artefacts are saved
- Live searches via agents
- Automated & repeatable
- Memory as a ‘normal’ source
- Chain of evidence for improvement purposes

Wondershare PDFelement

Wondershare PDFelement

Acquire

THERE IS NO SILVER BULLET

- What if you need the full disk image after the fact?
- What if the customer changes their opinion and wants to go to court?

Wondershare PDFelement

Wondershare
PDFelement

Processing

https://www.mentalfloss.com/article/645658/forensic-science-of-hair-analysis-flawed

Wondershare
PDFelement

Wondershare PDFelement

Processing

CURRENT STATE

- Unstructured string based (not always)
- Structured parsing into unstructured formats (not always)
- Slow, error prone, analyst required
- Closed source 'magical' information extraction
  - FTK
  - OpenText EnCase
- Non-repeatable due to intensive note taking required
  - Or grep your command line history
- Exportability & transferability are not easy

Wondershare PDFelement

Wondershare PDFelement

Processing

DESIRED STATE

- Structured parsing into structured formats
- Automated plugin-based processing pipelines
- Fast & scalable, no analyst required
- Transparent & inspectable operations
- Repeatable & deterministic
    - How else can we pinpoint bugs & solve them?
- Multi-source inputs should be a breeze

Wondershare PDFelement

Wondershare PDFelement

Processing

THERE IS NO SILVER BULLET

- What if the automated parsing contains errors?
  - What if the old skool analyst misses the errors?
- How do we even know that we have errors?
- Where are the public datasets?

Wondershare PDFelement

Analysis

https://www.kingston.ac.uk/postgraduate/courses/forensic-science-msc/

Wondershare PDFelement

Wondershare PDFelement

Wondershare PDFelement

Analysis

CURRENT STATE

- Single person focused
- Collaboration difficult
- Based on ‘human’ non-transferable knowledge
- Limited by difficult to extend analysis environment ‘Excel’

Wondershare PDFelement

Wondershare PDFelement

Analysis

DESIRED STATE

- Automated analysis on available data
- Human knowledge should feed into plugins & code
- Collaboration should be the default
    - Including real-time customer access
- Tools should be ‘easily’ extendable
- Findings should be repeatable

Wondershare PDFelement

Wondershare PDFelement

Analysis

THERE IS NO SILVER BULLET

- We still need human, but we should focus them on:
  - Doing the creative part
  - Doing the research part
- How do we prevent humans fully trusting the automated analysis?
- How do we detect, catch & remediate erroneous analysis?
  - Is this any different than applying this for human analysis?

Wondershare PDFelement

Wondershare PDFelement

Open-Source Software Incident Response Automation

Wondershare PDFelement

https://connect.redhat.com/en/blog/leading-automation-0

Wondershare PDFelement

Incident Response lab

PRINCIPLES

What we want

- Scalability
- Elasticity
- Availability
- Collaboration

What we do not want

- Scale a single system
- Dependent on a single system, disk or network share
- Downtime
- *“Hey can you share that spreadsheet with me?”*

Wondershare PDFelement

Wondershare PDFelement

Acquire

DESIRED STATE

- Forensics packages
  - Acquire based on forensic artefacts
  - Automated and scalable
- Tools: Velociraptor/Dissect Acquire
  - EDR using Live Response (all remote)

Wondershare PDFelement

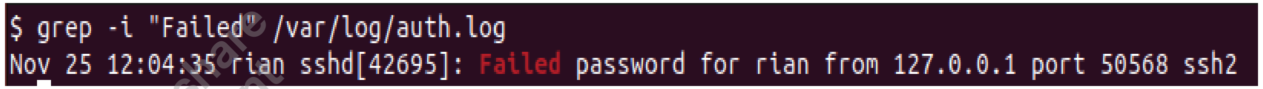
This Photo by Unknown Author is licensed under CC BY-SA

Wondershare
PDFelement

Unstructured Data

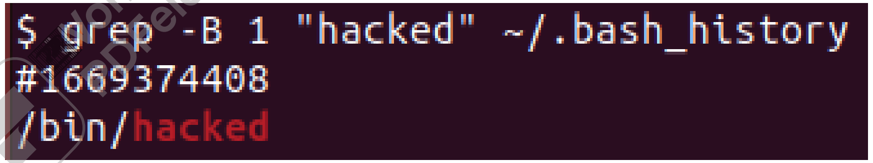
CURRENT STATE

- Authentication logs (user logons)



```
$ grep -i "Failed" /var/log/auth.log
Nov 25 12:04:35 rian sshd[42695]: Failed password for rian from 127.0.0.1 port 50568 ssh2
```

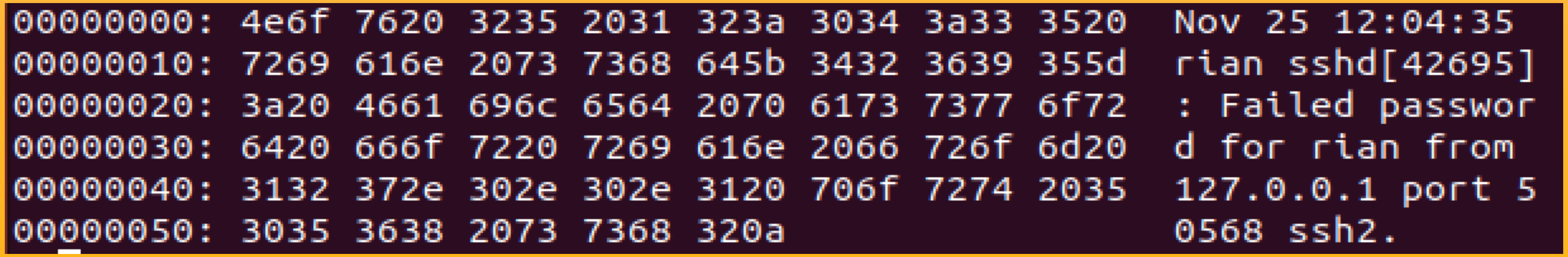
- Bash History (executed commands)



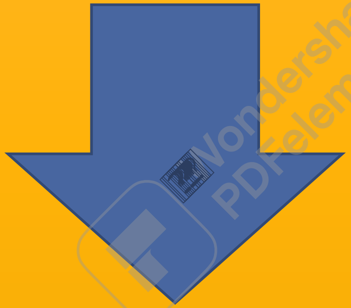
```
$ grep -B 1 "hacked" ~/.bash_history
#1669374408
/bin/hacked
```

Wondershare
PDFelement

Wondershare
PDFelement



```
00000000: 4e6f 7620 3235 2031 323a 3034 3a33 3520  Nov 25 12:04:35
00000010: 7269 616e 2073 7368 645b 3432 3639 355d  rian sshd[42695]
00000020: 3a20 4661 696c 6564 2070 6173 7377 6f72  : Failed passwor
00000030: 6420 666f 7220 7269 616e 2066 726f 6d20  d for rian from
00000040: 3132 372e 302e 302e 3120 706f 7274 2035  127.0.0.1 port 5
00000050: 3035 3638 2073 7368 320a                 0568 ssh2.
```

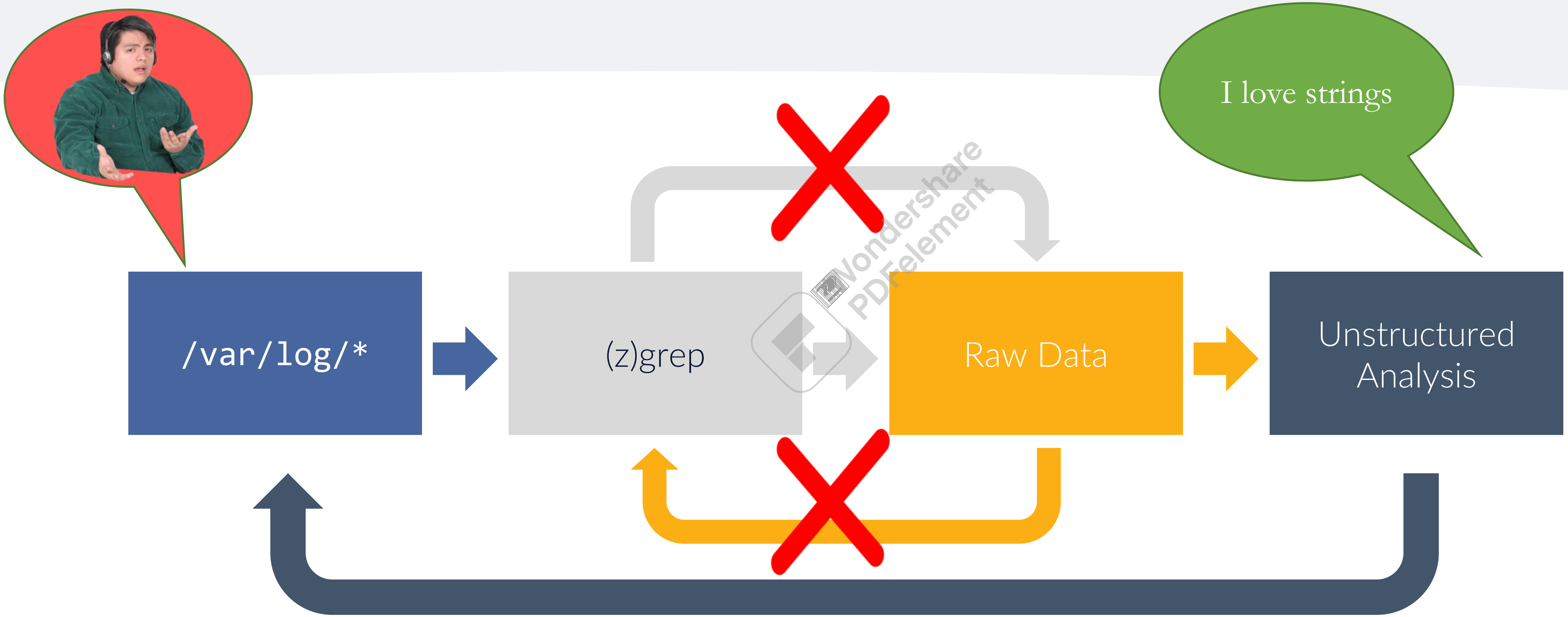


Wondershare
PDFelement

```
timestamp:’29/11/2022 13:58’ user:rian ip:127.0.0.1 action:login result:failed
timestamp:’29/11/2022 13:58’ user:rian ip:127.0.0.1 action:login result:failed
timestamp:’29/11/2022 13:58’ user:rian ip:127.0.0.1 action:login result:failed
timestamp:’29/11/2022 13:59’ user:rian ip:127.0.0.1 action:login result:successful session_id:1
timestamp:’29/11/2022 14:00’ user:rian command:”/bin/hacked” shell:/bin/bash
```

Wondershare
PDFelement

Big picture

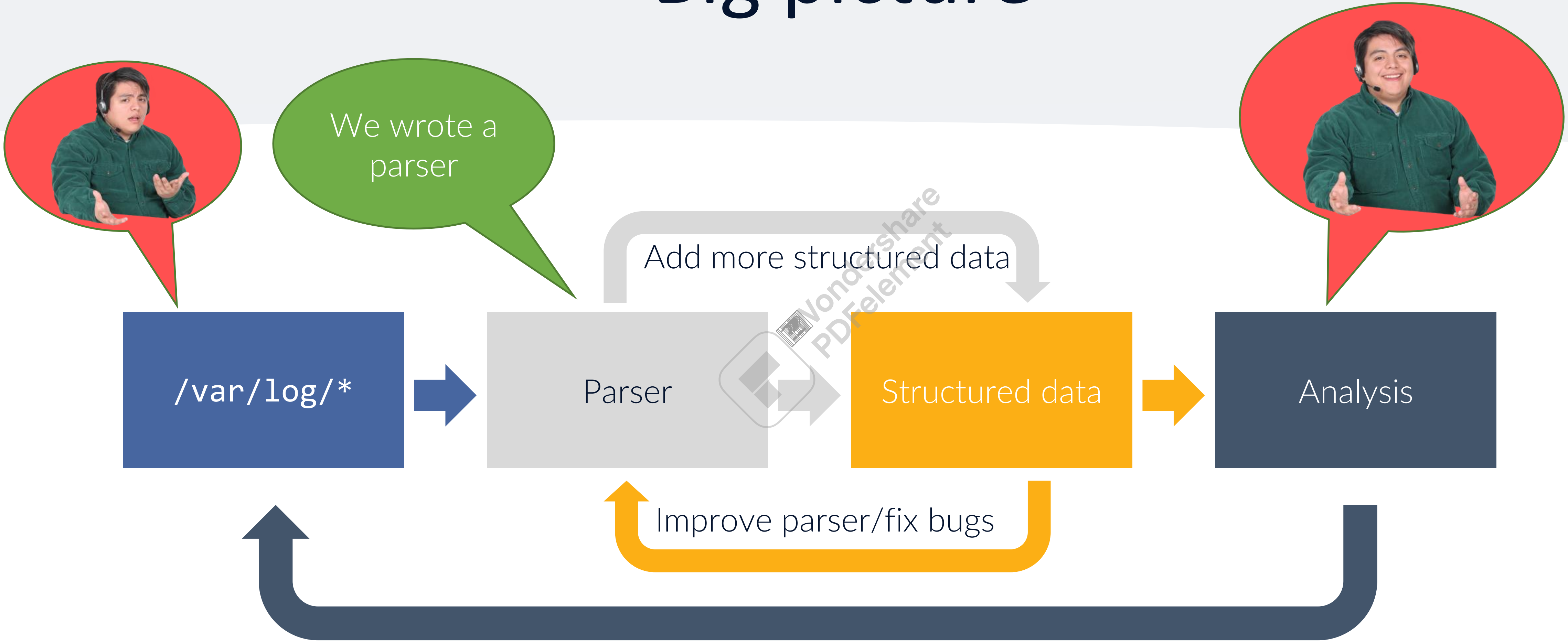


Wondershare
PDFelement

New incident - repeating manual steps over and over again

Wondershare
PDFelement

Big picture



New incident ☺

Wondershare
PDFelement

Wondershare PDFelement

Analysis

DESIRED STATE

- Timelines, timelines, timelines
- Query language
  - `srcip:127.0.0.1 AND srcport:1337`
- Backup
  - GNU tools: `strings, grep, awk, cut, etc.`

Wondershare PDFelement

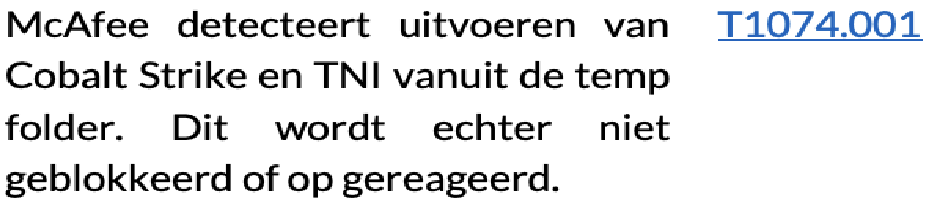
Wondershare PDFelement

Automated Analysis

SHOW IT

- Repeatable
- Transform human knowledge

Wondershare PDFelement



McAfee detecteert uitvoeren van Cobalt Strike en TNI vanuit de temp folder. Dit wordt echter niet geblokkeerd of op gereageerd. T1074.001

```
data_type:"windows:evtx:record" AND
source_name:McLogEvent           AND
event_identifier:257
```

https://www.huntandhackett.com/redmudnester, https://github.com/huntandhackett/red-mudnester/blob/main/RedMudnester.ipynb

Wondershare
PDFelement

DevOps Mindset

CHALLENGE

Automation

Feedback Loops

Iterative

Repeatability

Speed

Metrics

Continuous Improvement

Structured Data

Wondershare
PDFelement

Wondershare PDFelement

We would like to thank YOU!

Wondershare PDFelement

Wondershare
PDFelement

Acquire

Wondershare
PDFelement

Wondershare PDFelement

Acquire

Process

Wondershare PDFelement

Wondershare PDFelement

Acquire

gsutil cp

Beats

Process

Logstash

Analysis

timesketch

elasticsearch

jupyter

sigma

Wondershare PDFelement

PUBLIC

HUNT & HACKETT

EVOLVE YOUR INCIDENT RESPONSE

Share your thoughts

Wondershare PDFelement

Wondershare PDFelement