EDINBURGH
JUNE 16-21
2019

Seeing Clearly and Communicating Effectively to Address Event Overload

Thomas V Fischer

FVT SecOps Consulting

TLP:WHITE

I am …

- Security Advocate & Threat Researcher focused on Data Protection
- 25+ years' experience in InfoSec
- Spent number years in corporate IR team positions

- BSidesLondon Director
- ISSA UK – VP of Data Governance

- Contact
  - tvfischer+sec@gmail.com tvfischer@tvf-prod.com (secure email)
  - @Fvt
  - keybase.io/fvt

Learning from 1st Responder Lessons Learnt

- Communications issues
- Self dispatching & recall
- Lack of accountability
- Unclear chain of command
- Uncertain roles/task assignments

Thanks to Chris Sutherland (ING) for these references

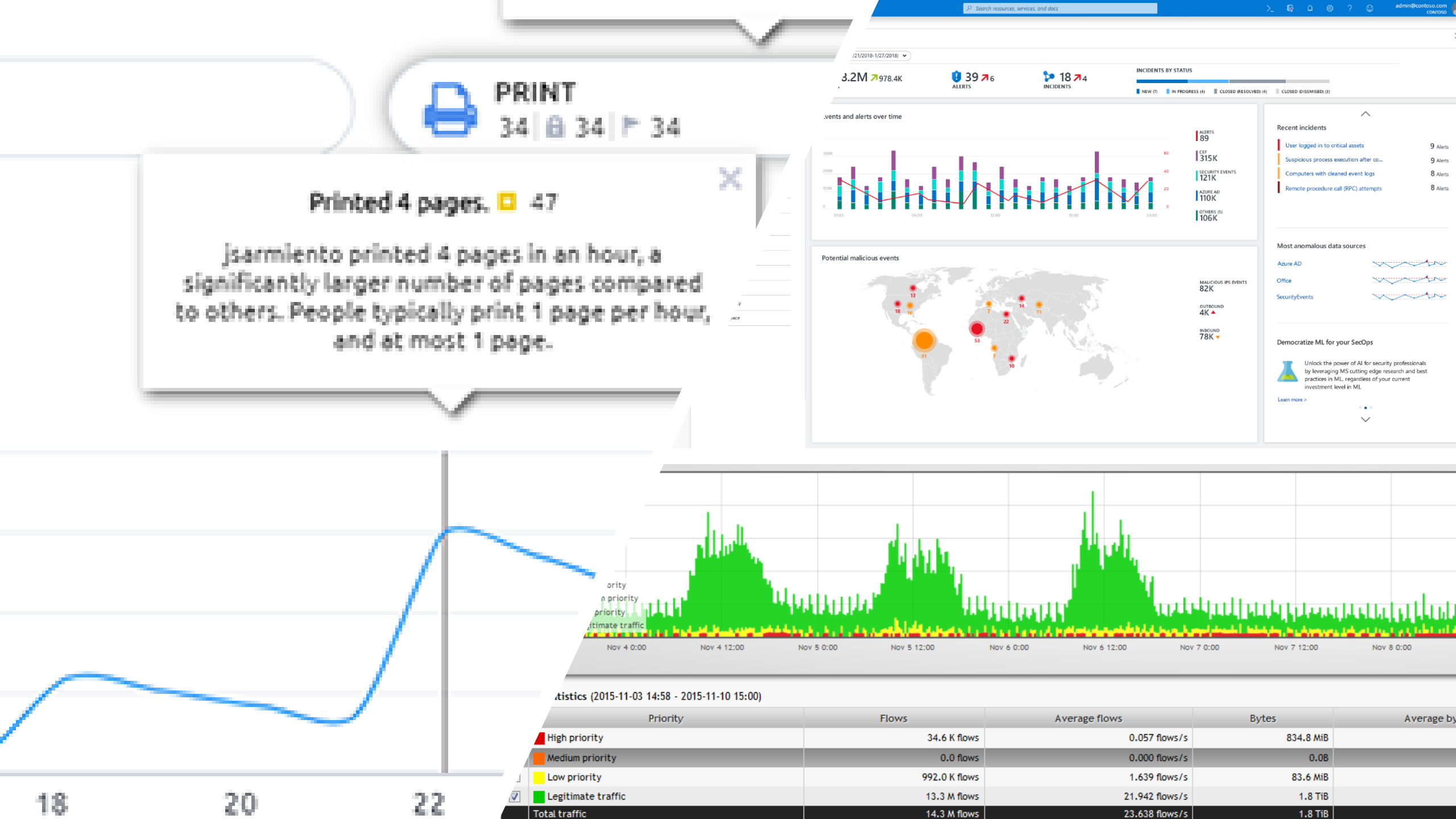
Communication Issues

- × Unclear if units received dispatch instructions
- × Portable radio limitations
- × 10 different Call Codes
- × Lack of situational awareness
- × Structural collapse
- × Many firefighters and officers in tower 1 unaware of tower 2 collapse

TLP:WHITE

Visualization enables an analyst to gain an overview of data during an investigation

Schrenk and Poisel, 2011


PRINT
34 34 34
Printed 4 pages. 47
jsarmiento printed 4 pages in an hour, a significantly larger number of pages compared to others. People typically print 1 page per hour, and at most 1 page.
Search resources, services, and docs
admin@contoso.com
CONTOSO
3.2M 978.4K
ALERTS
39 6
INCIDENTS
18 4
INCIDENTS BY STATUS
NEW (7)
IN PROGRESS (4)
CLOSED (RESOLVED) (4)
CLOSED (DISMISSED) (3)
.vents and alerts over time
ALERTS 89
CEF 315K
SECURITY EVENTS 121K
AZURE AD 110K
OTHERS (5) 106K
Recent incidents
User logged in to critical assets 9 Alerts
Suspicious process execution after co... 9 Alerts
Computers with cleaned event logs 8 Alerts
Remote procedure call (RPC) attempts 8 Alerts
Potential malicious events
MALICIOUS IPS EVENTS 82K
OUTBOUND 4K
INBOUND 78K
Most anomalous data sources
Azure AD
Office
SecurityEvents
Democratize ML for your SecOps
Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML
Learn more >
18
20
22
ority
priority
priority
timate traffic
Nov 4 0:00
Nov 4 12:00
Nov 5 0:00
Nov 5 12:00
Nov 6 0:00
Nov 6 12:00
Nov 7 0:00
Nov 7 12:00
Nov 8 0:00
tistics (2015-11-03 14:58 - 2015-11-10 15:00)
Priority
Flows
Average flows
Bytes
Average by
High priority 34.6 K flows 0.057 flows/s 834.8 MiB
Medium priority 0.0 flows 0.000 flows/s 0.0B
Low priority 992.0 K flows 1.639 flows/s 83.6 MiB
Legitimate traffic 13.3 M flows 21.942 flows/s 1.8 TiB
Total traffic 14.3 M flows 23.638 flows/s 1.8 TiB

- Matching IOC
- Signature Based

- Security/Hunting Analytics
- Stats Methods
- Start of UEBA

Predictive IR

- Supervised machine learning
- Incorporate previous signals

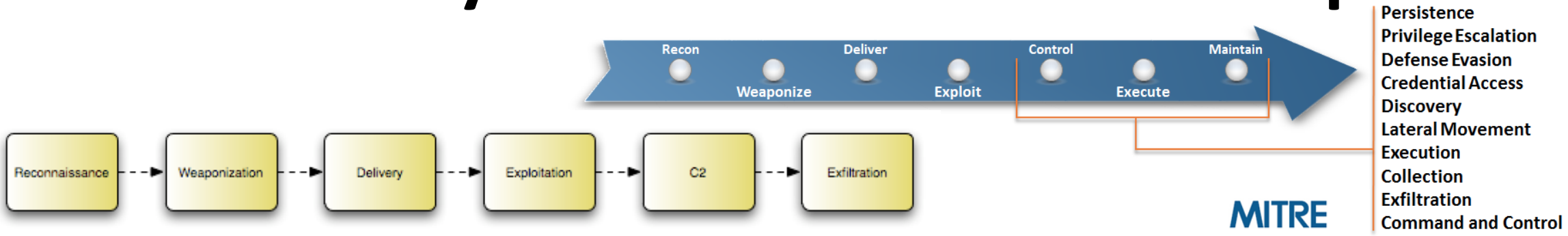
Proactive IR

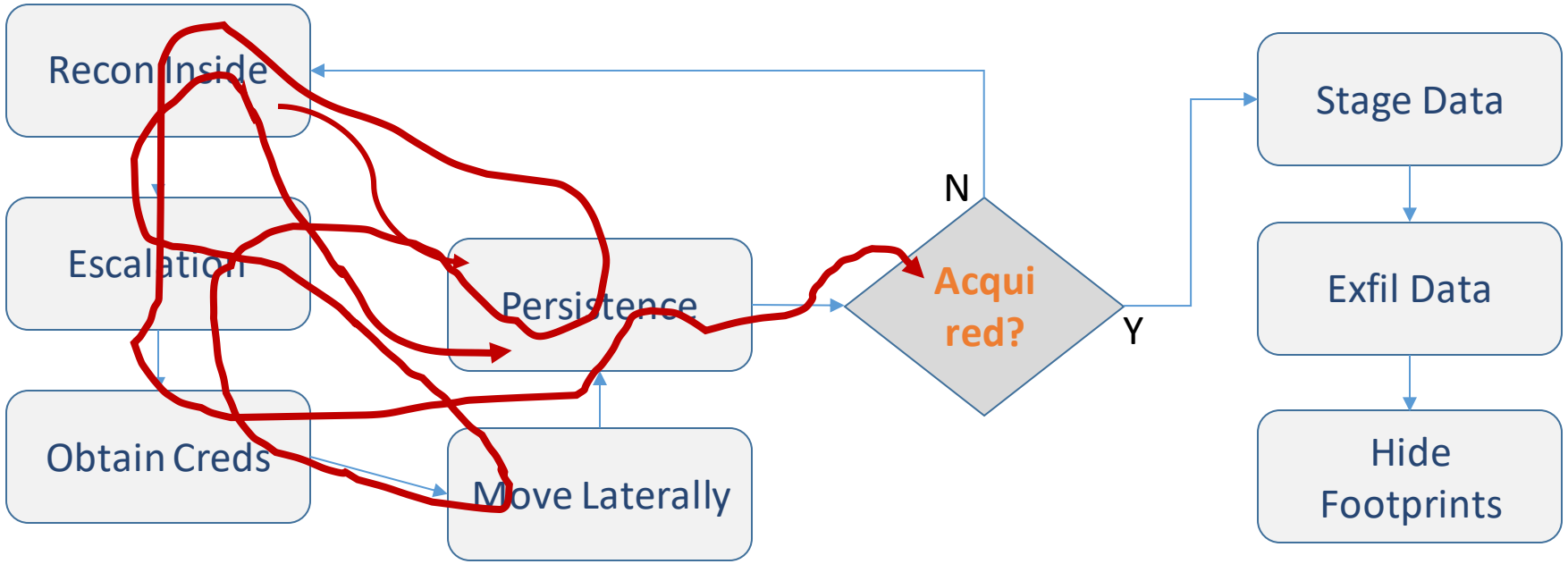
HUMAN

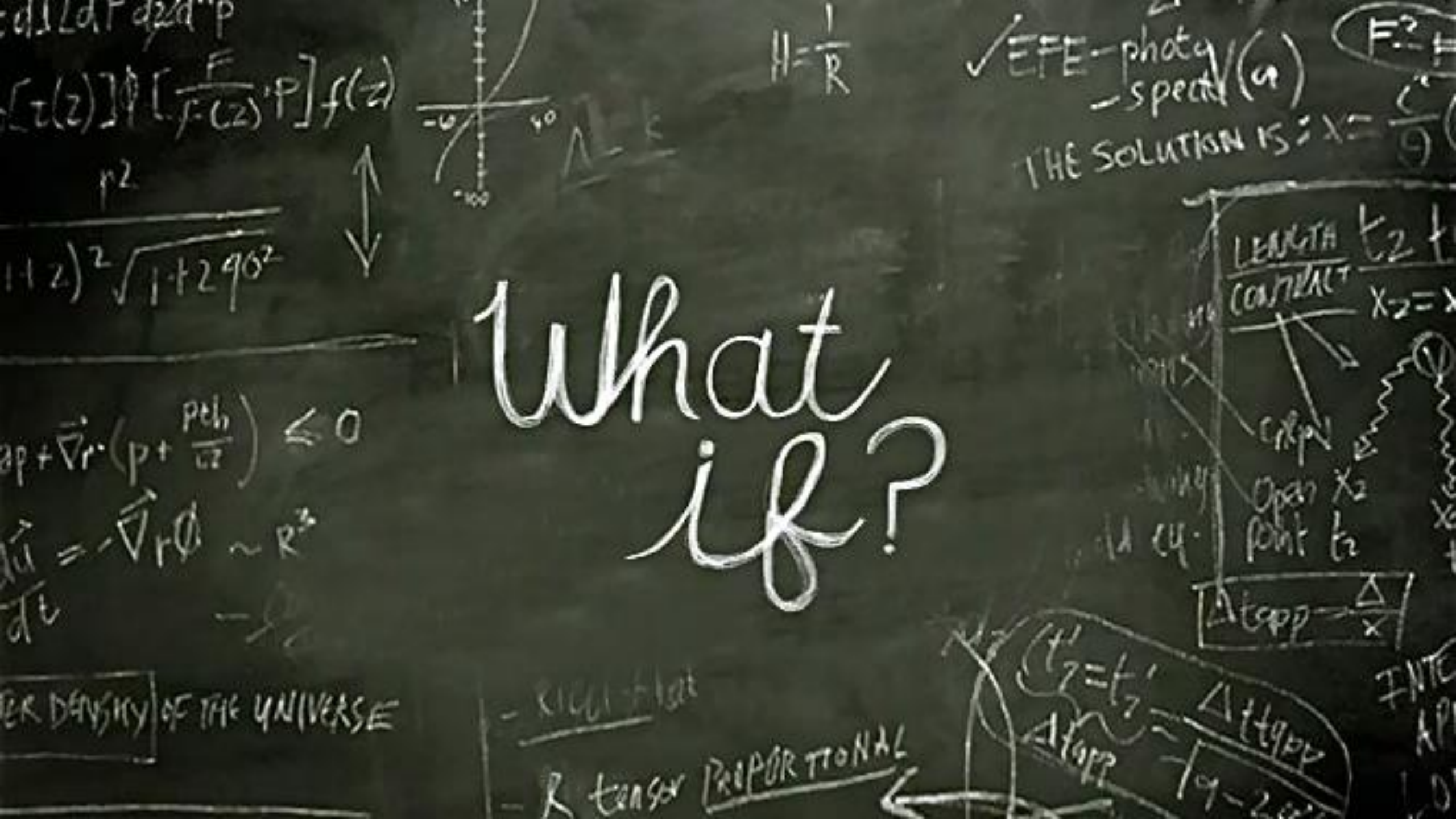
Thanks to Alex Pinto

C… 17 techn…					…dential Access 14 techniques	Execution 30 techniques, 6 used	Lateral Movement 15 techniques	Collection 11 techniques	Exfiltration 9 techniques	Delivery 3 techniques
Commonly Used Port		…Manipulation…	Manipulation	…ount Discovery	Account Manipulation	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Background Inte… Service
Communication Through Removable Media	Accessibility Features	Binary Padding	Accessibility Features	Application Window Discovery	Bash History	Application Shimming	Application Deployment Software	Automated Collection	Data Compressed	Archived Payloa…
Connection Proxy	AppInit DLLs	Bypass User Account Control	AppInit DLLs	File and Directory Discovery	Brute Force	Command-Line Interface	Exploitation of Vulnerability	Clipboard Data	Data Encrypted	Maldocs
Custom Command and Control Protocol	Application Shimming	Clear Command History	Application Shimming	Network Service Scanning	Create Account	Execution through API	Logon Scripts	Data Staged	Data Transfer Size Limits	
Custom Cryptographic Protocol	Authentication Package	Code Signing	Bypass User Account Control	Network Share Discovery	Credential Dumping	Execution through Module Load	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	
Data Encoding	Bootkit	Component Firmware	DLL Injection	Peripheral Device Discovery	Credentials in Files	Graphical User Interface	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	
Data Obfuscation	Change Default File Association	Component Object Model Hijacking	DLL Search Order Hijacking	Permission Groups Discovery	Exploitation of Vulnerability	InstallUtil	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	
Fallback Channels	Component Firmware	DLL Injection	Dylib Hijacking	Process Discovery	Input Capture	Launchctl	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	
Multi-Stage Channels	Component Object Model Hijacking	DLL Search Order Hijacking	Exploitation of Vulnerability	Query Registry	Input Prompt	PowerShell	Remote Services	Input Capture	Scheduled Transfer	
Multiband Communication	Cron Job	DLL Side-Loading	File System Permissions Weakness	Remote System Discovery	Keychain	Process Hollowing	Replication Through Removable Media	Screen Capture		
Multilayer Encryption	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information	Launch Daemon	Security Software Discovery	Network Sniffing	Regsvcs/Regasm	Shared Webroot	Video Capture		
Remote File Copy	Dylib Hijacking	Disabling Security Tools	Local Port Monitor	System Information Discovery	Private Keys	Regsvr32	Taint Shared Content			
Standard Application Layer Protocol	External Remote Services	Exploitation of Vulnerability	New Service	System Network Configuration Discovery	Securityd Memory	Rundll32	Third-party Software			
Standard Cryptographic Protocol	File System Permissions Weakness	File Deletion	Path Interception	System Network Connections Discovery	Two-Factor Authenticatio… Interception					
Standard Non-Application Layer Protocol	Hidden Files and Directories	File System Logical Offsets	Plist Modification	System Owner/User Discovery						
Uncommonly Used Port	Hypervisor	Gatekeeper Bypass	Scheduled Task	System Service Discovery						

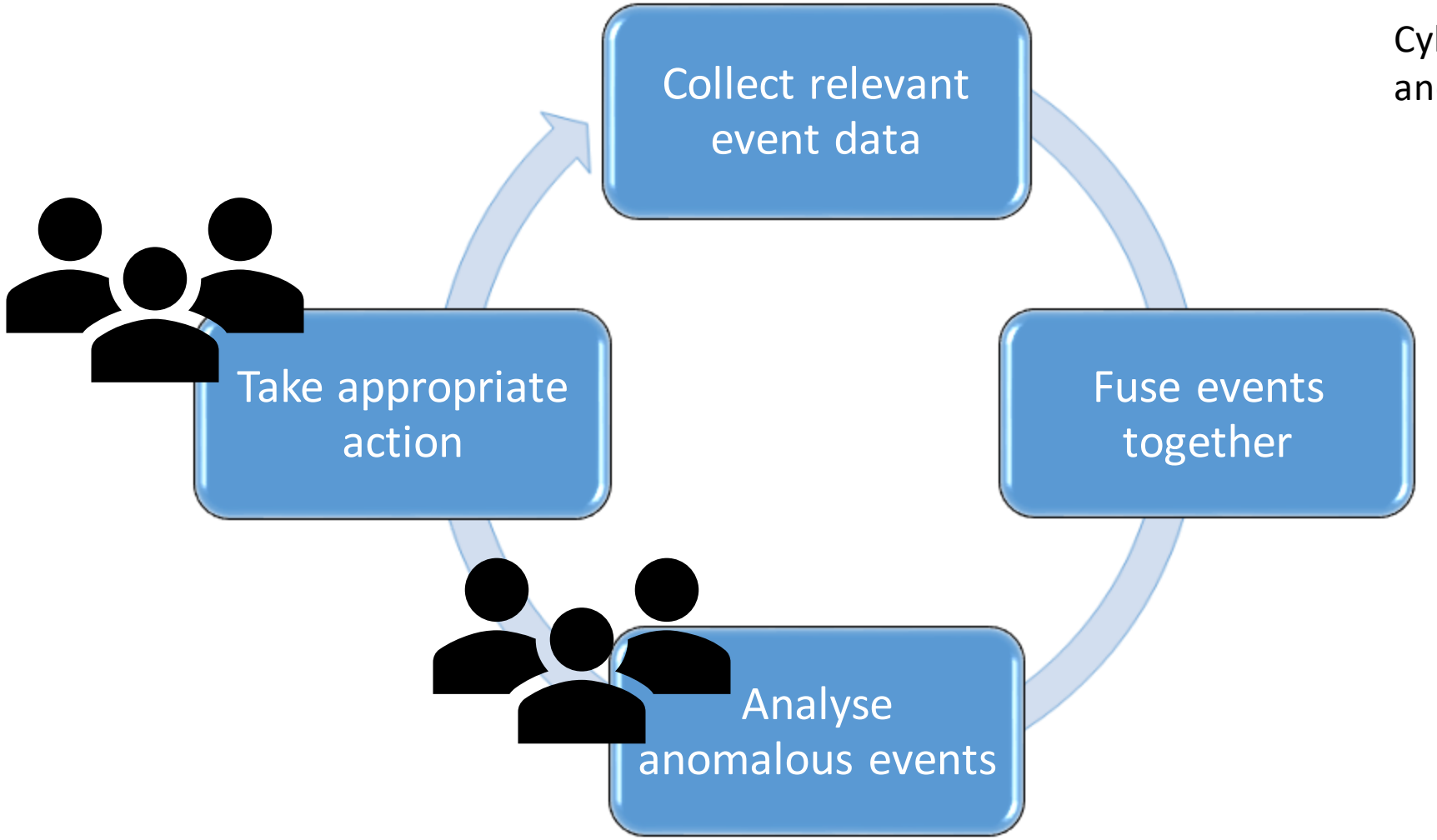
Orientation by Framework – Does it Help?






What if?

Key Phases in the Monitoring Process



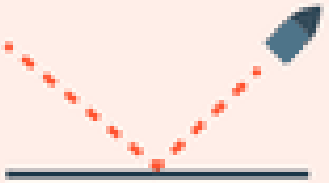
Cyber Security Monitoring and Logging Guide

CREST

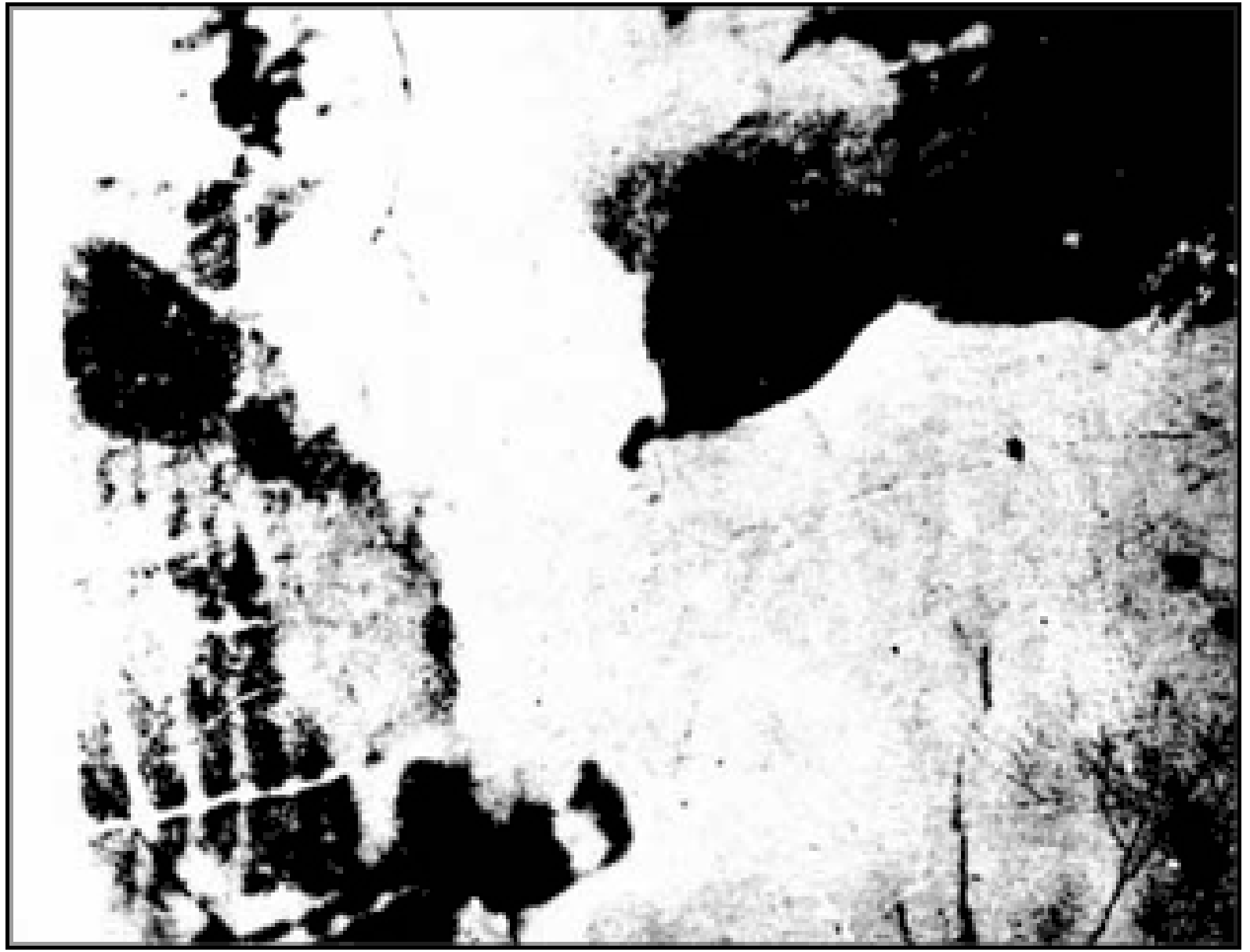

iz not stalking... just
intently staring
ICANHASCHEEZBURGER.COM

The type of weapon used

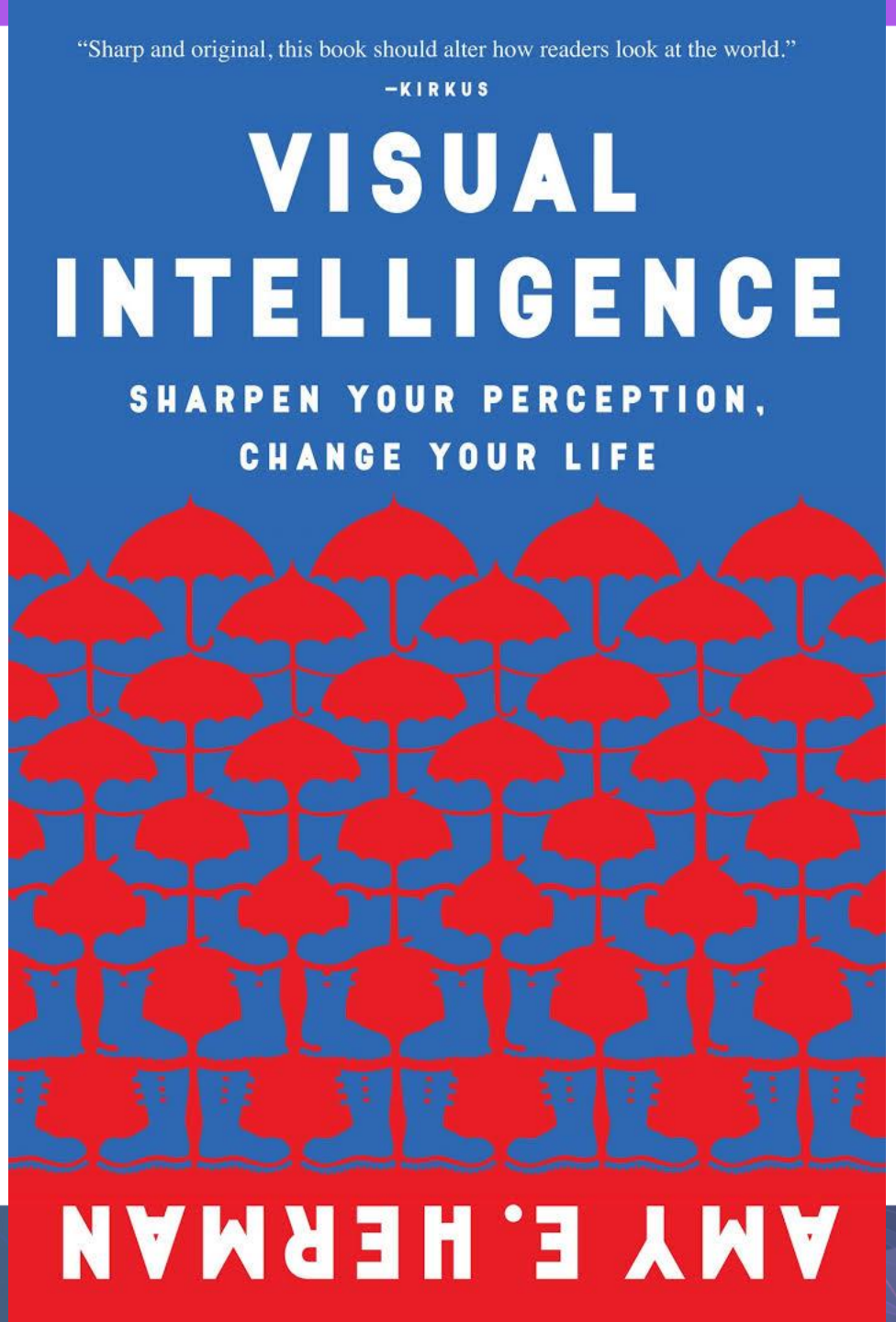
The direction of travel of a victim or suspect

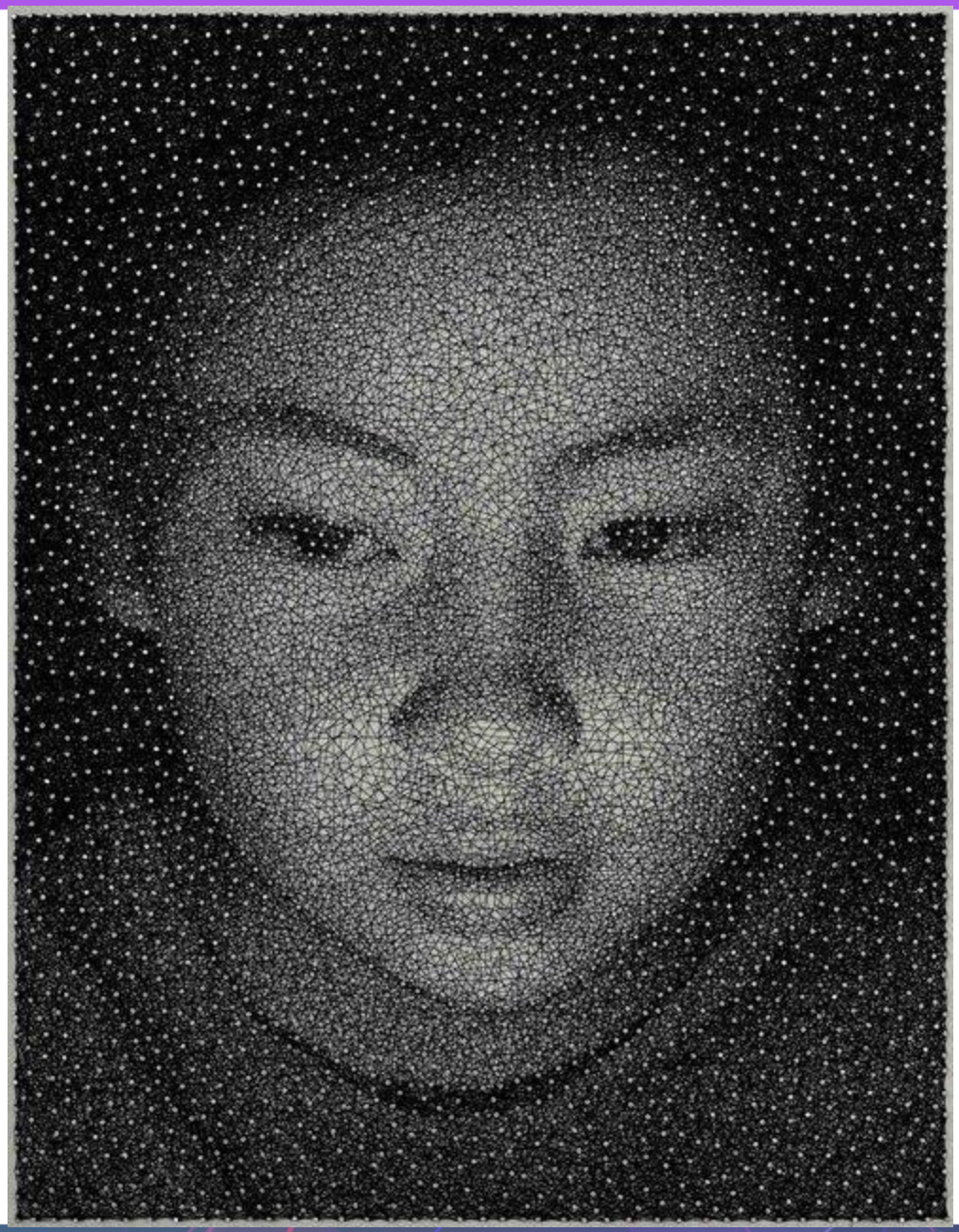


Trajectory of a projectile



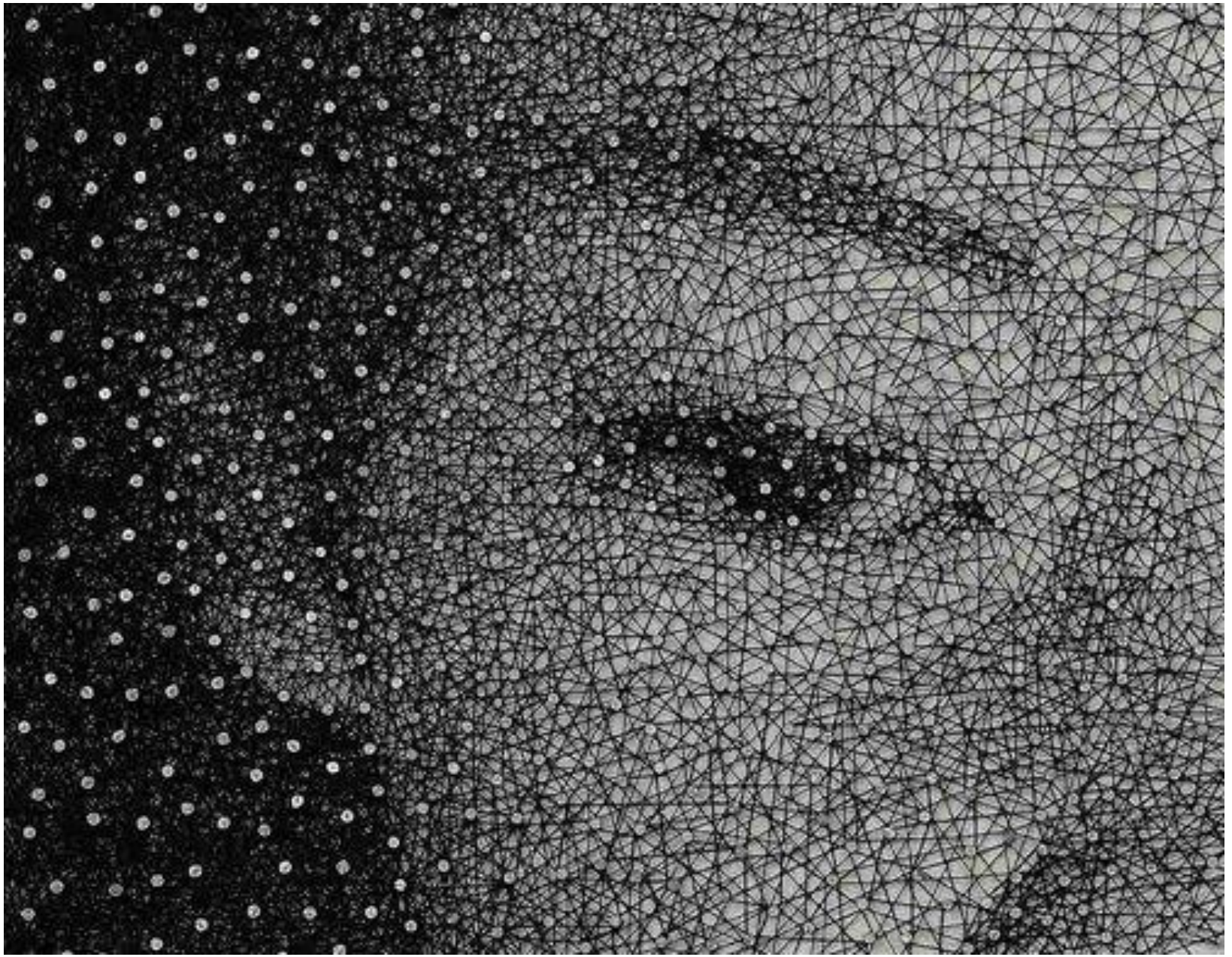
TLP:WHITE


"Sharp and original, this book should alter how readers look at the world."
—KIRKUS
VISUAL INTELLIGENCE
SHARPEN YOUR PERCEPTION, CHANGE YOUR LIFE
AMY E. HERMAN

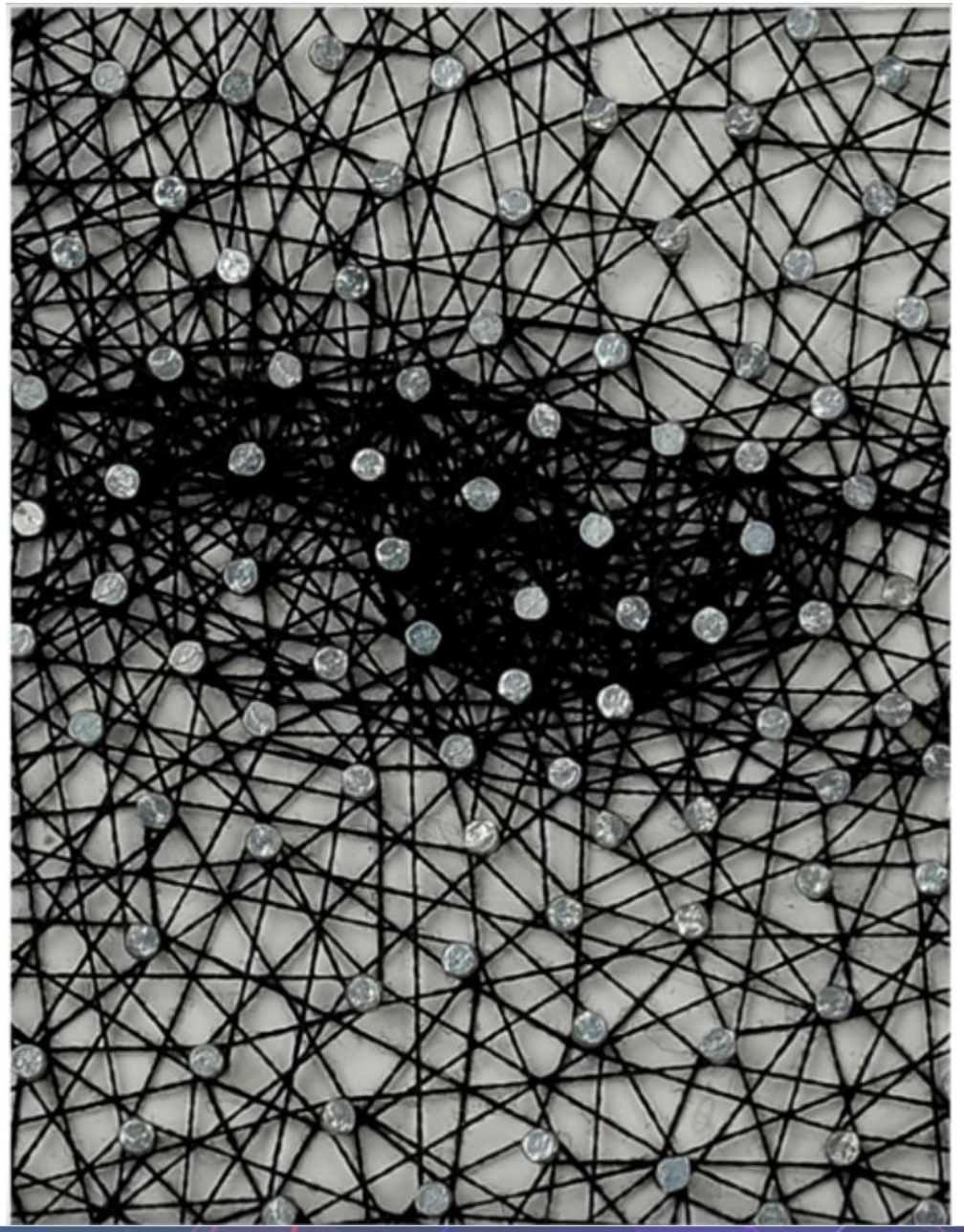


Portrait by Kumi Yamashita

TLP:WHITE



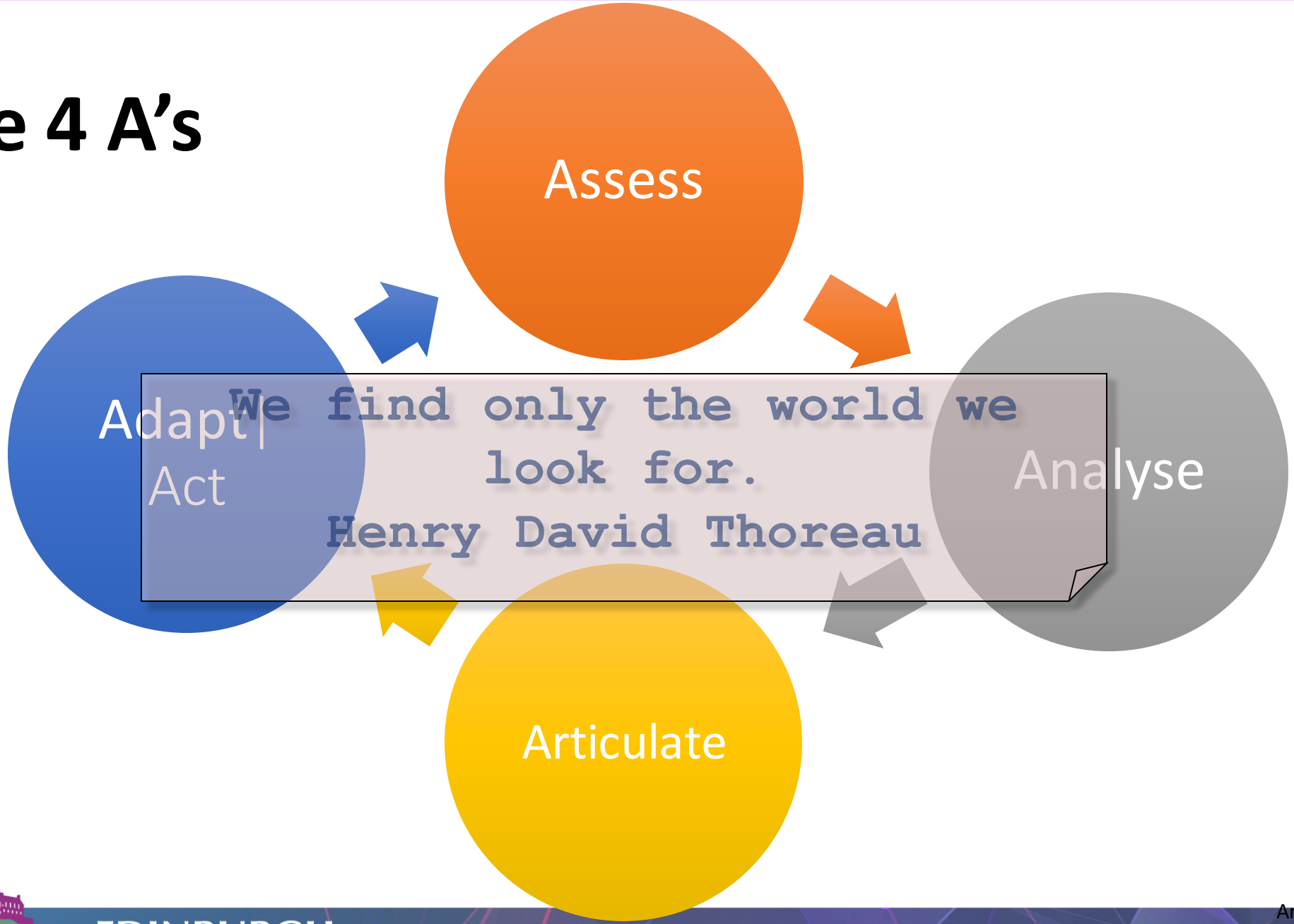
What is this Work of Art?



- Is it a painting?
- Is it a sculpture?
- What is it made of?

Learning to frame the question to elicit the information to do our jobs

The 4 A's



Amy Herman, *The Art of Perception*

Something Gets Lost

- Effective break down between what we see down to what we communicate
- Ability to translate what we wee to others
- Talk about complicated situations to simple situations

Assess

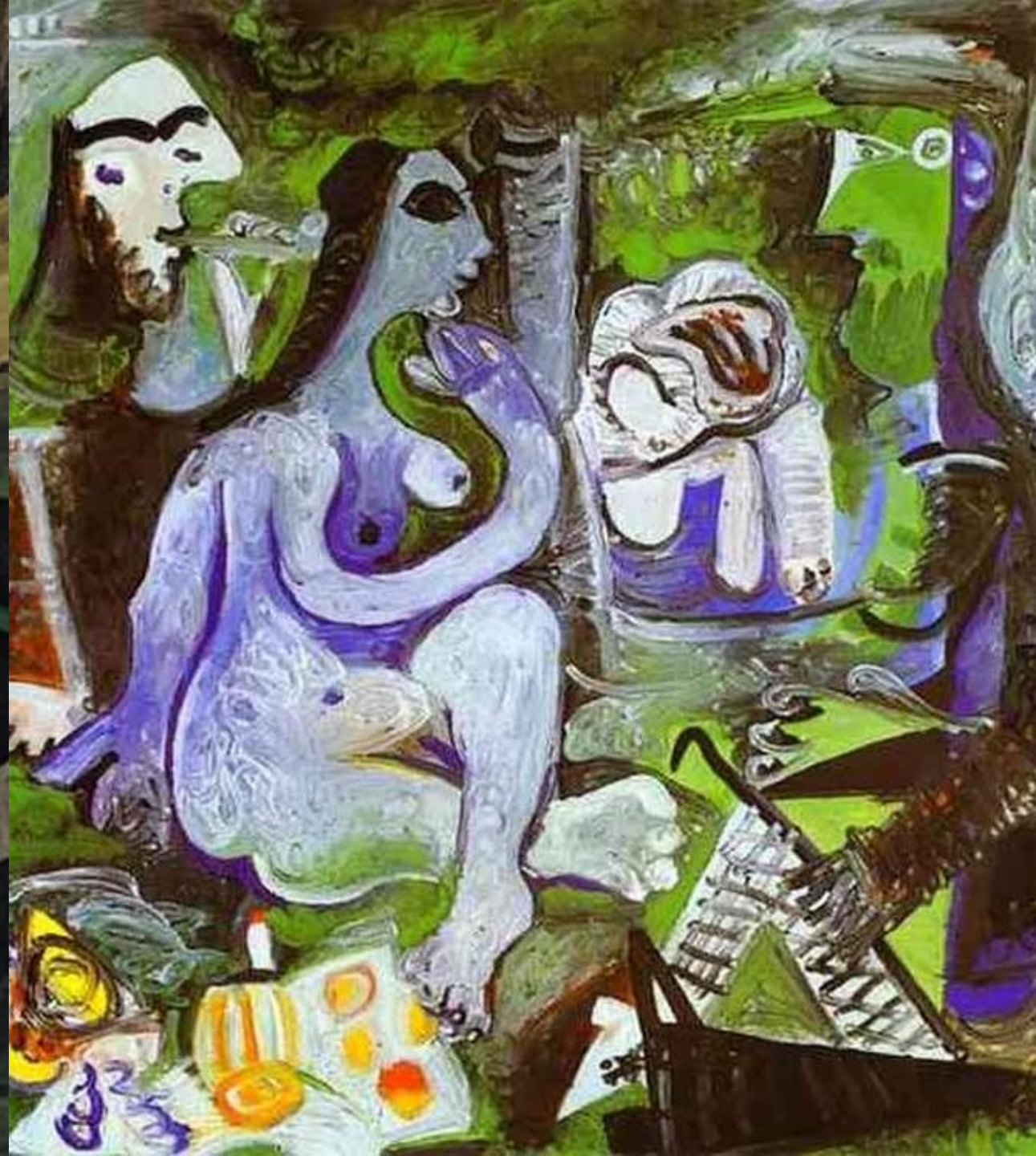
What is in Front of Us

Study Thoroughly

`saper vedere`

No Two People See the Same Way

"Luncheon on the Grass" by Manet 1863



Count how many times the players wearing white pass the ball

The Monkey Business Illusion

- So what was the

Analyse

What is important?

What do I need?

What don't I need?

Analyse the elements observed

Inattentional blindness

Articulate

Articulate the facts succinctly

Remove assumptions

Also what don't you see

Assumptions
Danger! Danger!

Explain what you have seen and communicate it

Adapt

Perspective

Formulate questions to address the seeming inconsistencies

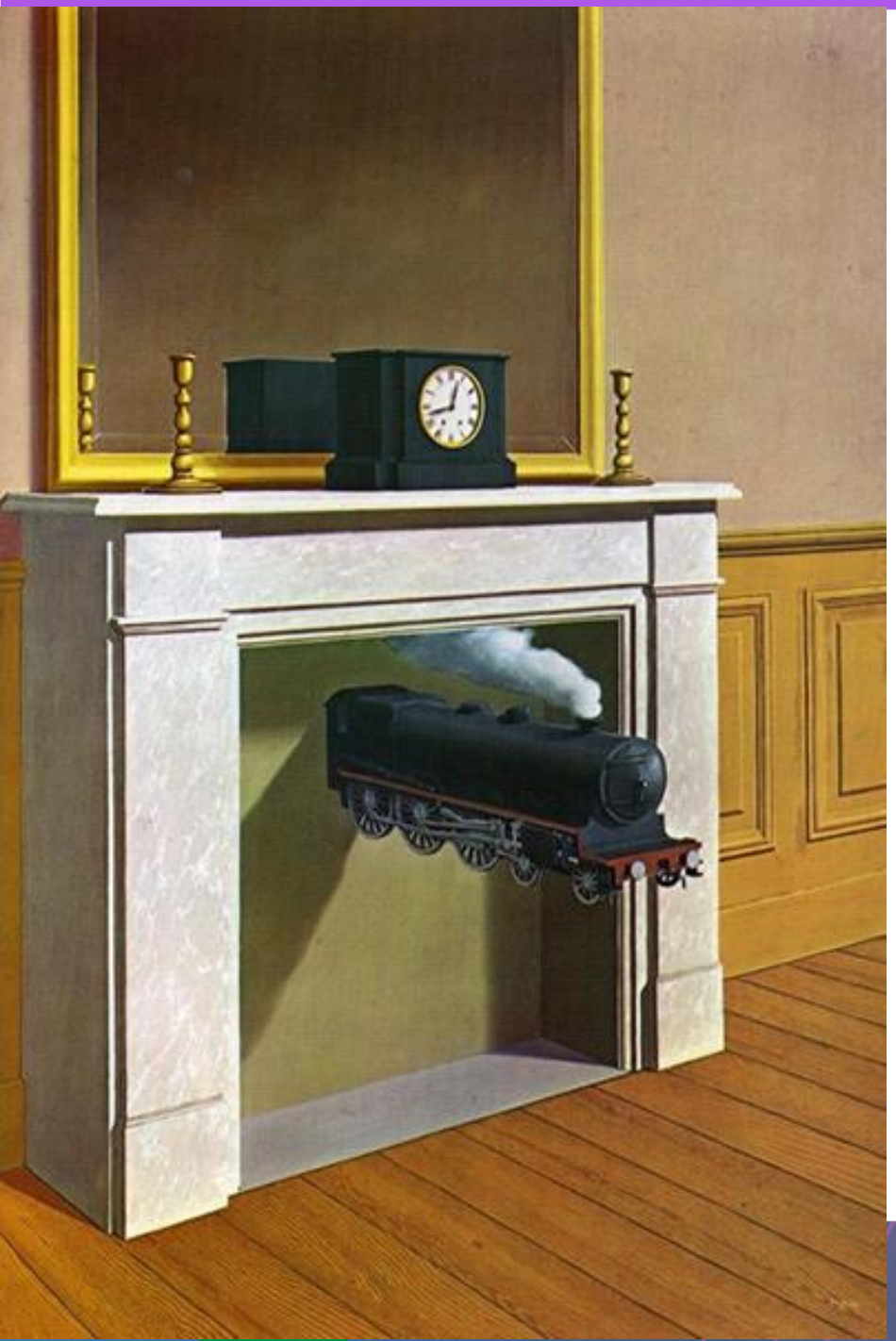
Observations inform perceptions and perceptions inform inferences

Step back take another look

Take an Action Based on What we See and Communicate

Did you see …

Renshaw's Cow



Summarise the picture

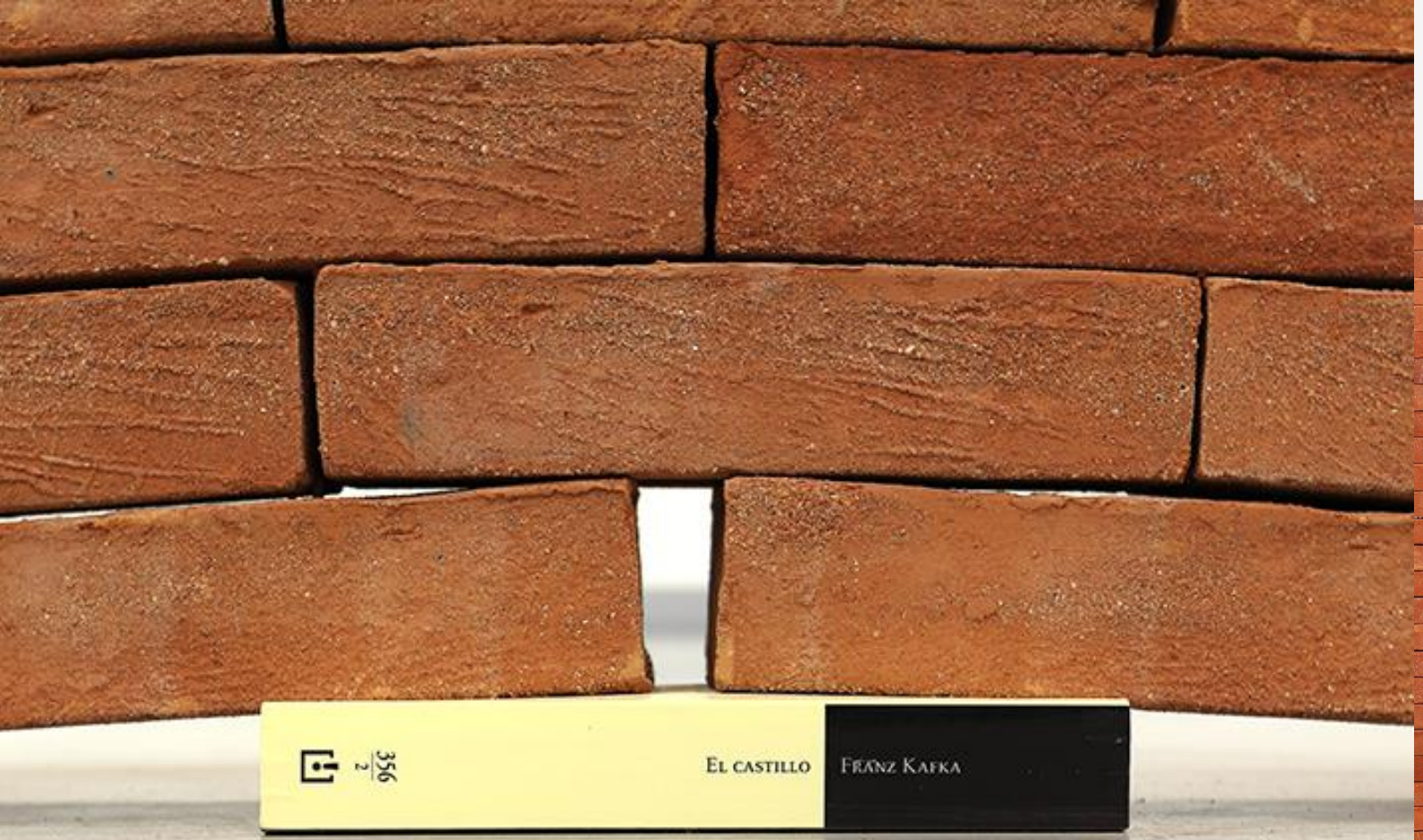
But what did you leave out?

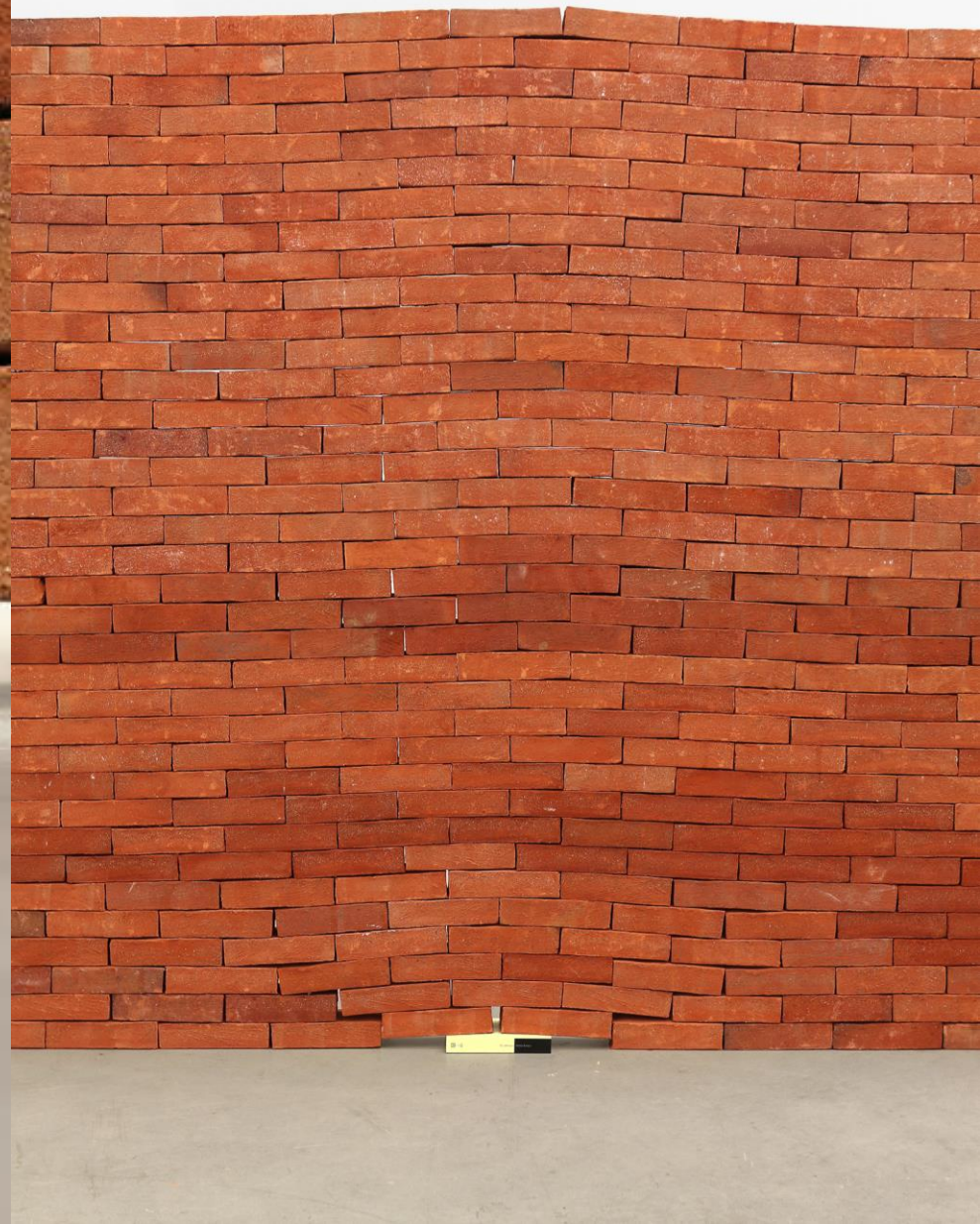
René Magritte Time Transfixed

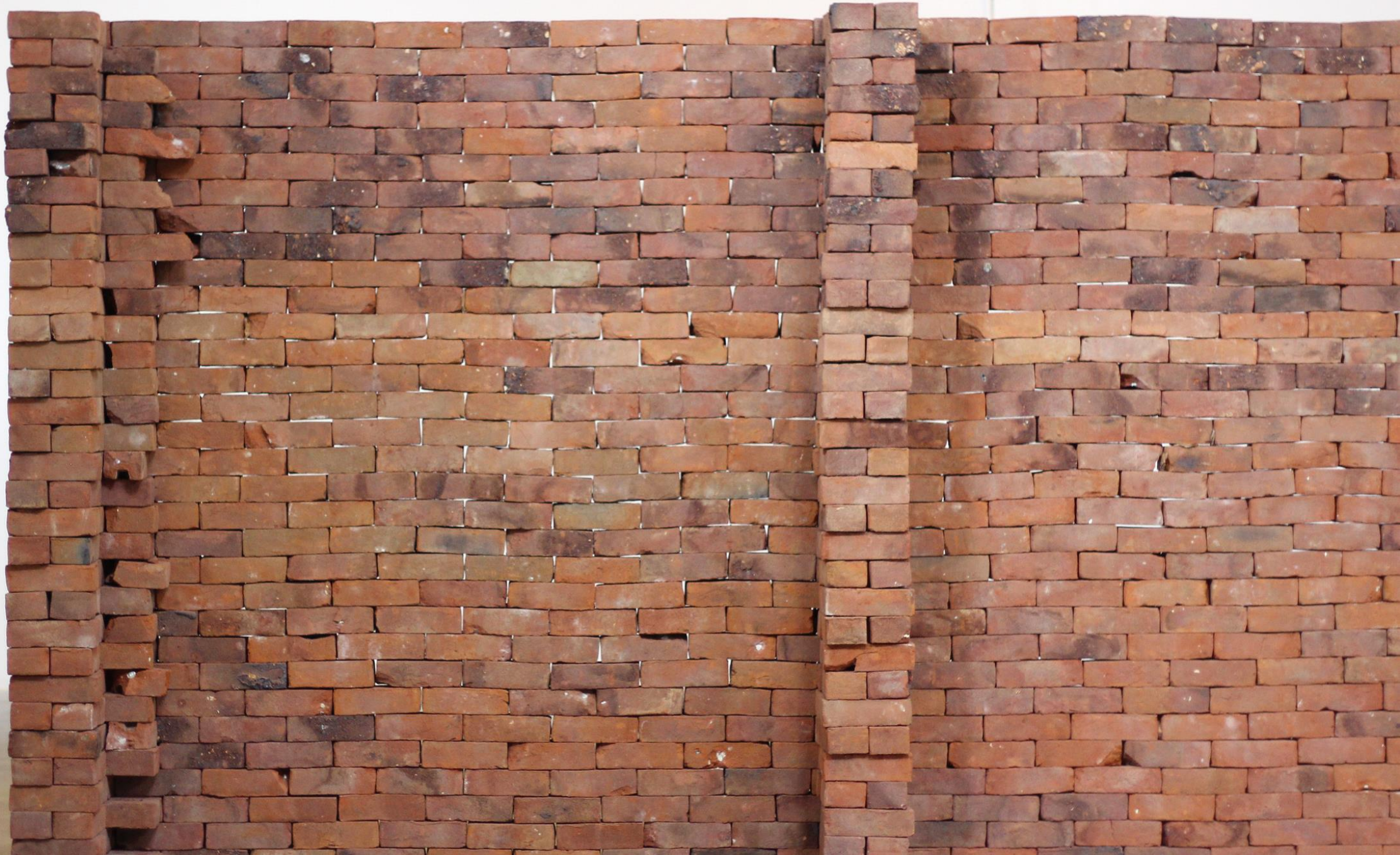
TLP:WHITE

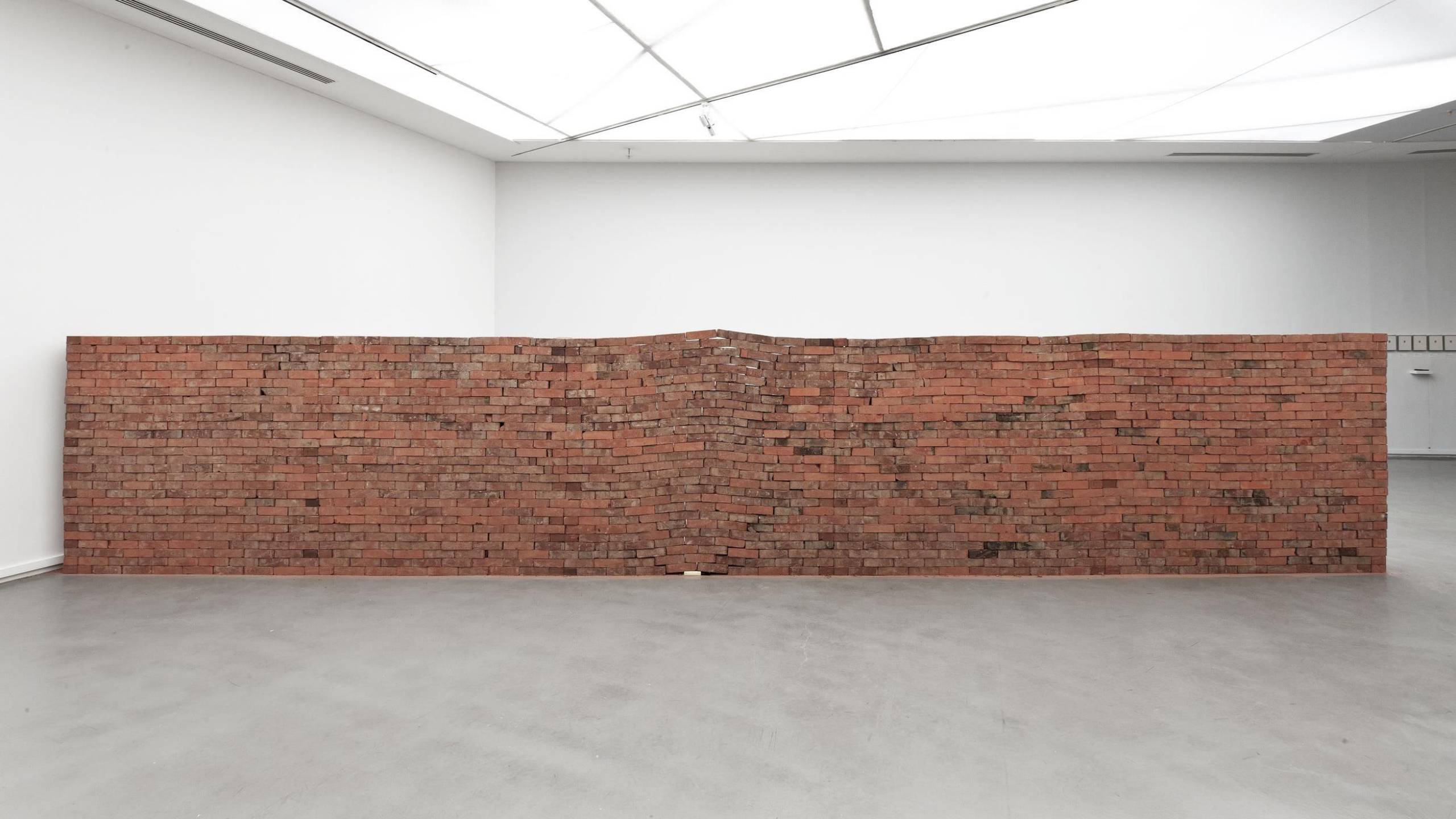
Giuseppe Arcimboldo - The Vegetable Gardener

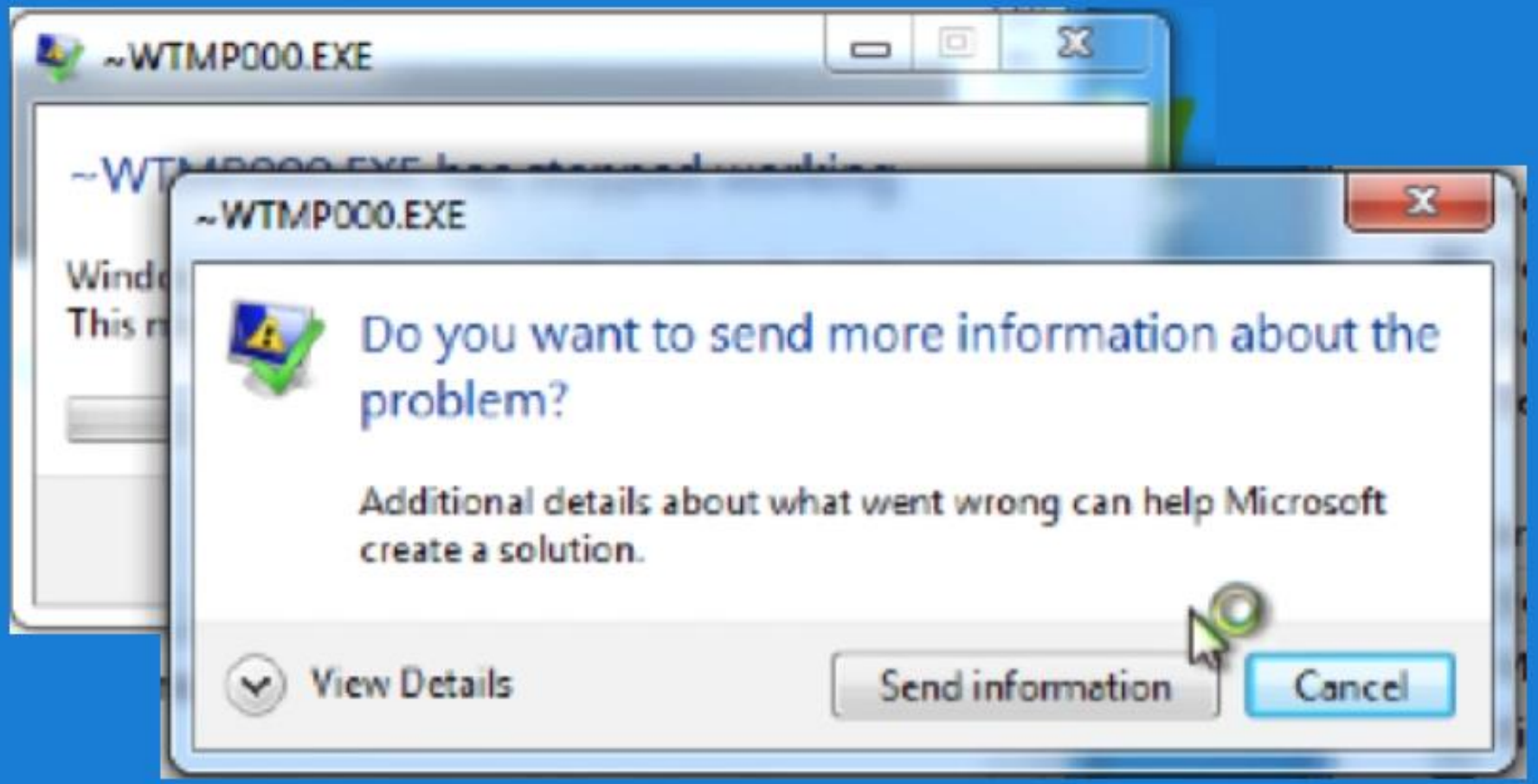
El castillo de Jorge Méndez Blake

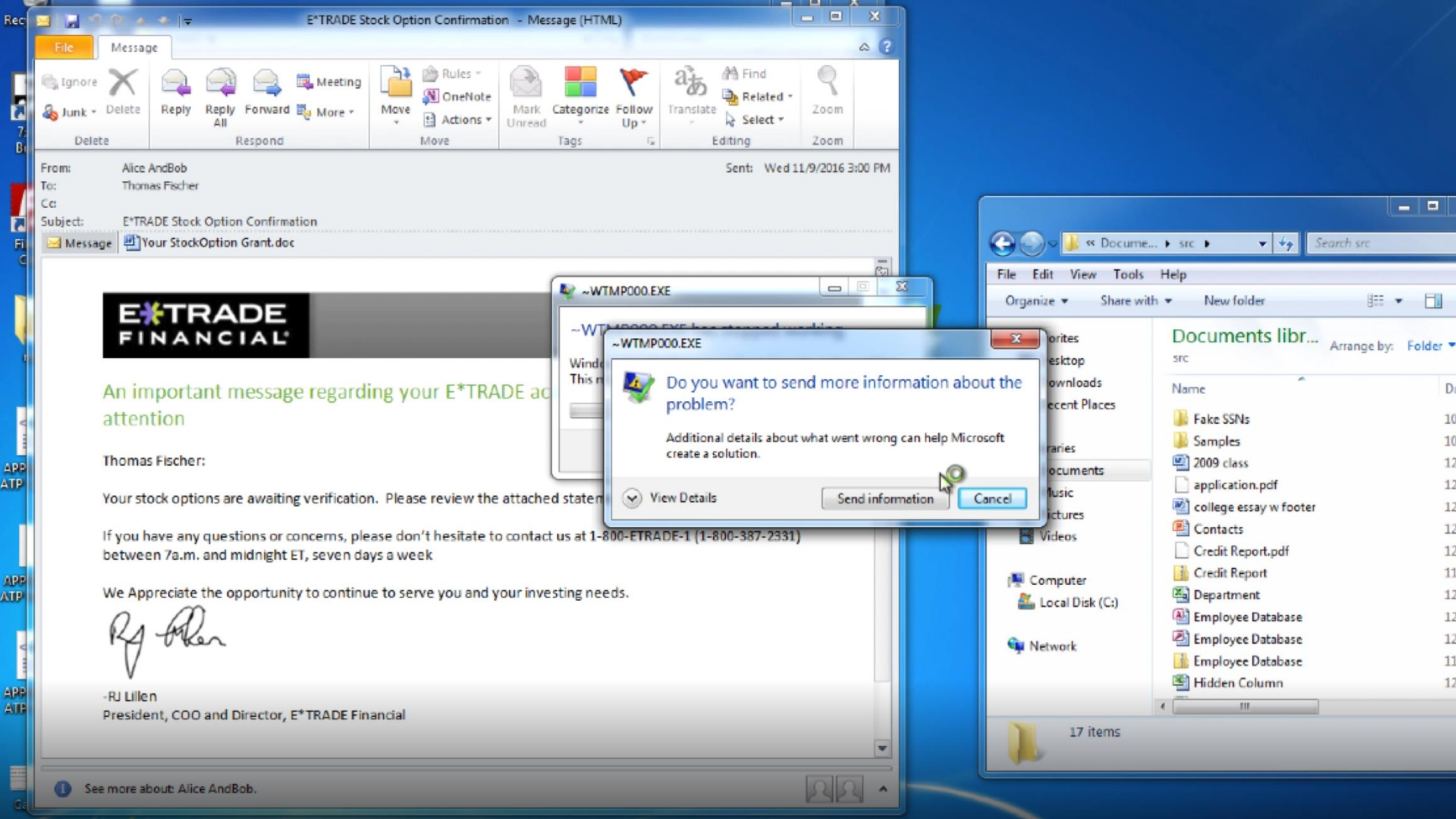









~WTMP000.EXE
~WTMP000.EXE
Do you want to send more information about the problem?
Additional details about what went wrong can help Microsoft create a solution.
View Details
Send information
Cancel


E*TRADE Stock Option Confirmation - Message (HTML)
File
Message
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Move
Rules
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Move
Tags
Editing
Zoom
From: Alice AndBob
To: Thomas Fischer
Cc:
Subject: E*TRADE Stock Option Confirmation
Sent: Wed 11/9/2016 3:00 PM
Message
Your StockOption Grant.doc
E*TRADE FINANCIAL
An important message regarding your E*TRADE ac
attention
Thomas Fischer:
Your stock options are awaiting verification. Please review the attached staten
If you have any questions or concerns, please don't hesitate to contact us at 1-800-ETRADE-1 (1-800-387-2331) between 7a.m. and midnight ET, seven days a week
We Appreciate the opportunity to continue to serve you and your investing needs.
-RJ Lillen
President, COO and Director, E*TRADE Financial
See more about: Alice AndBob.
~WTMP000.EXE
~WTMP000.EXE
Do you want to send more information about the problem?
Additional details about what went wrong can help Microsoft create a solution.
View Details
Send information
Cancel
File Edit View Tools Help
Organize
Share with
New folder
Search src
Documents libr...
src
Arrange by: Folder
Name
Fake SSNs
Samples
2009 class
application.pdf
college essay w footer
Contacts
Credit Report.pdf
Credit Report
Department
Employee Database
Employee Database
Employee Database
Hidden Column
Computer
Local Disk (C:)
Network
17 items

Contextual or Situational Awareness

Where are you now?

How do you proceed?

Are you comfortable about what you are seeing?

What else is around you?

What are the problems I am aware of?

Choice of words in both spoken and written language is important

Present Your Ideas

- In a way your reader can understand and build a picture
- Lead with the key fact, to
  - Seed your findings
  - Build a clear summary
- Begin with an action verb
- Highlight the impact

Keep it Succint

- Write a sentence
- Re-evaluate it
- Shorten it
- Get to the point faster

Be Precise

- Remove
  - Clutter
  - Assumptions
  - unnecessary/irrelevant details
- Highlight the important information

In Conclusion

Understand how you come across

both figuratively and literally!

There are things you are seeing that are right in front of your eyes...

Have you gone back and told your colleagues, and re-evaluated

how did I miss that?

It was right there?

In Conclusion
Collaborate

Here is my issue, here is my problem.

Is there something that I might be missing?

Do you know something that i don’t

In Conclusion

Don’t reach for what you want to see

Be accountable for you observations

Jump to a conclusion; document how you get there

"If you change the way you look at things, the things you look at change"

Dr. Wayne Dyer

@Fvt

› tvfischer+sec@gmail.com tvfischer@tvf-prod.com (secure)

› keybase.io/fvt