Cyber Forensics

Jorge Carrillo, PhD

20.02.2014

Chalmers University

Microsoft

Agenda

- ✓ Quick intro
- ✓ A typical Forensic Process
- ✓ Forensic and Incident Management
- ✓ Forensic in the EU
- ✓ Cyber-Forensic: Looking ahead.
- ✓ Wrapping up
- ✓ Q&A

If you could invest your time, energy for….

A) Building a device that will travel faster than light.

B) Selling a car that can travel only to the future

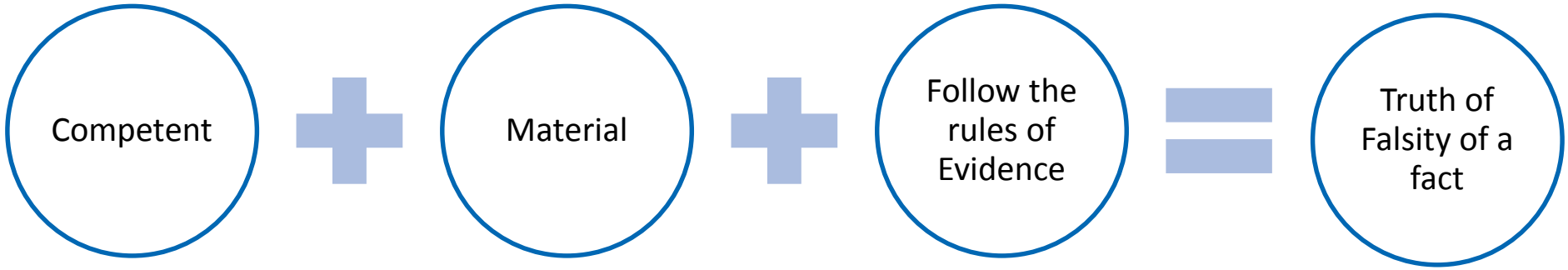
C) Mastering digital forensic methods and tools

What would you chose?.

Basic Principle

"Any action of an individual, and obviously the violent action constituting a crime, cannot occur without leaving a trace."

Key elements in forensic evidence

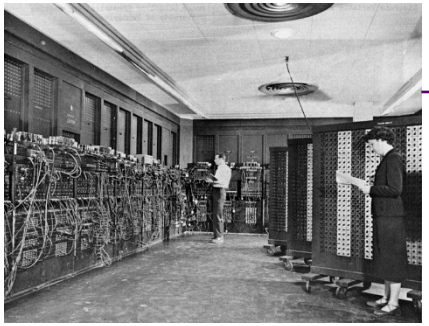


Type of Evidence

- Direct Evidence
- Real
- Documentary
- Demonstrative (second hand evidence)

Protect the chain of custody

IT Race



1945

35 years

1987

25 years

2012

2014

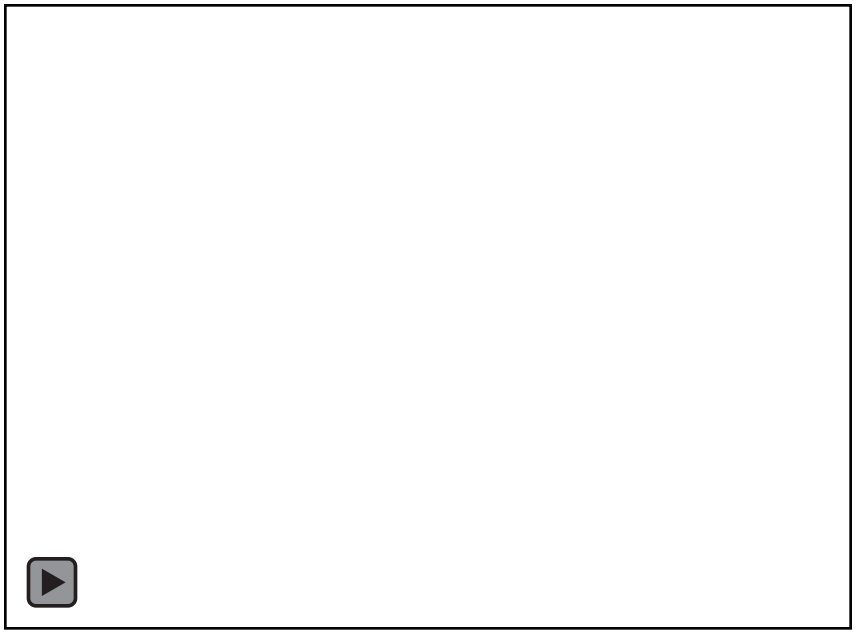
Key Changes:

- ✓ Focus on business, information and risk. (rather than technology only)
- ✓ Blending personal life with work life.
- ✓ IT does not own/control all the infrastructure.
- ✓ Not clear difference between external and internal infrastructure.
- ✓ Millions of malware being created, attacks expands in minutes.
- ✓ All the time on-line and everything connected.

Example: Challenge in data Analysis

…. I don't know what is happening, but whatever the position of my government is, I support it fully.

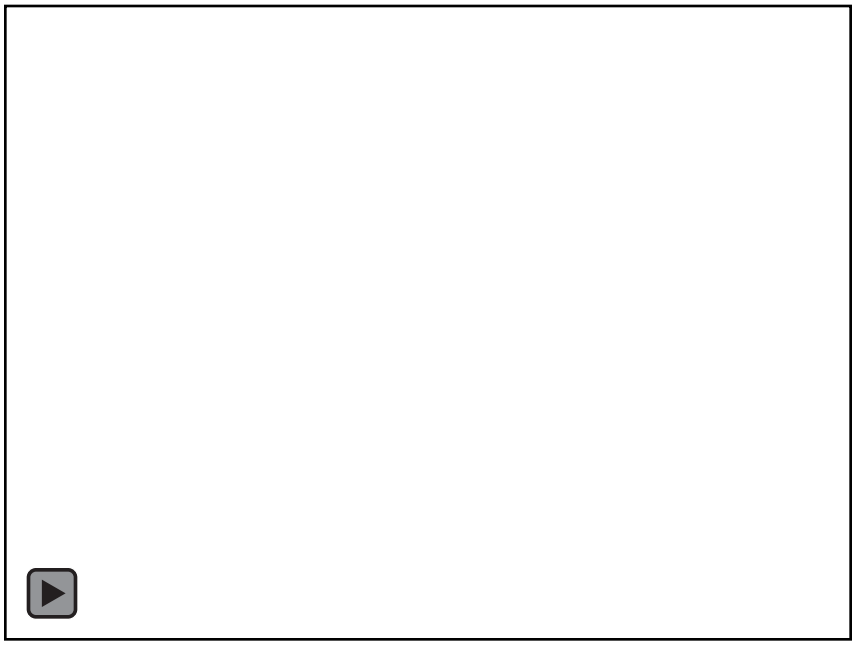
Whatever the position of my government, I believe in it, yes sir. I am a member of that government,…



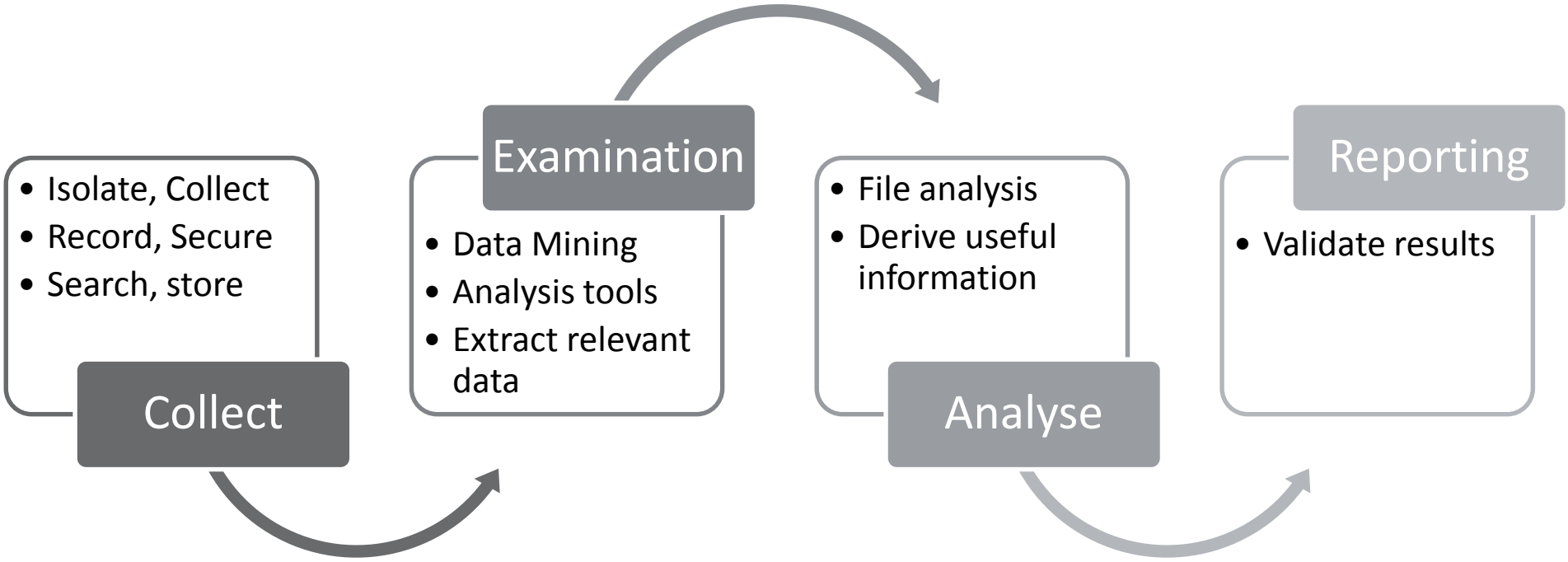
Example: How would you react to this situation?

…. No way!!!!…

I am getting hacked…

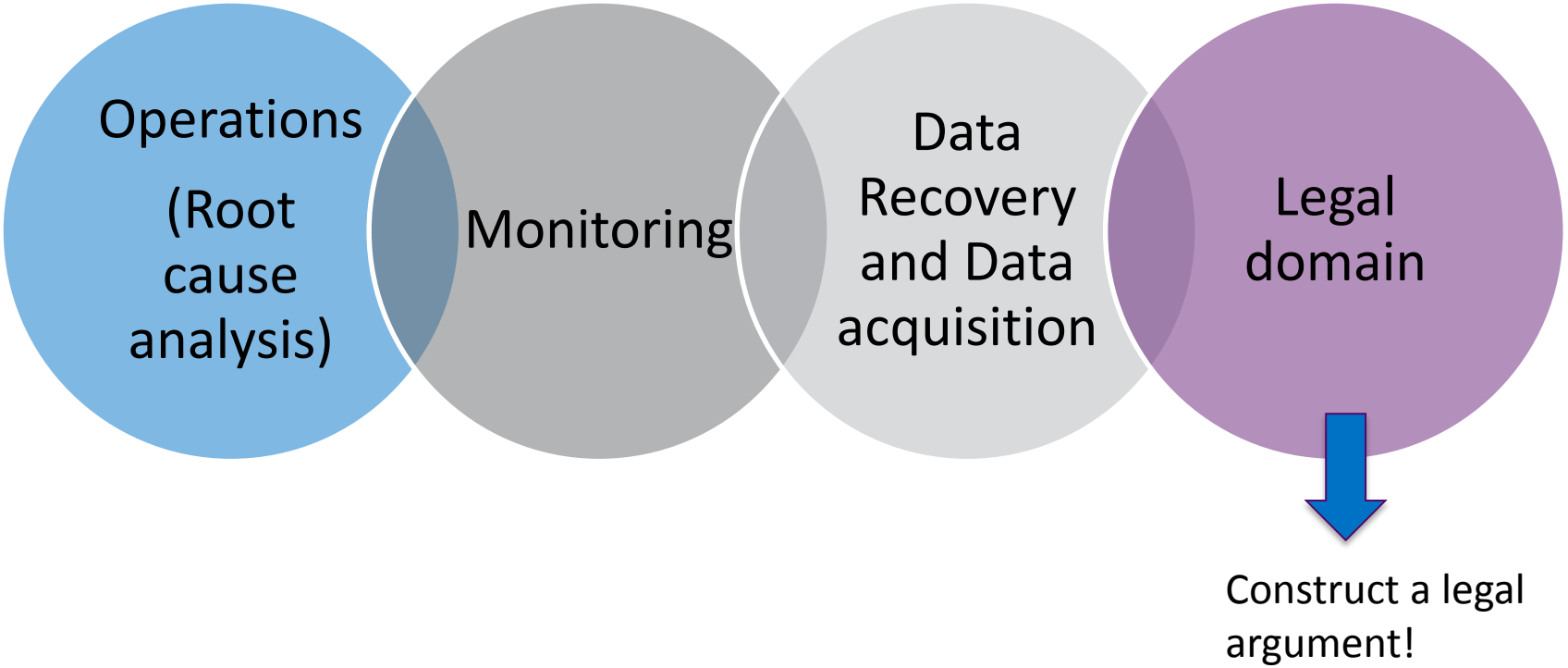


The right process…

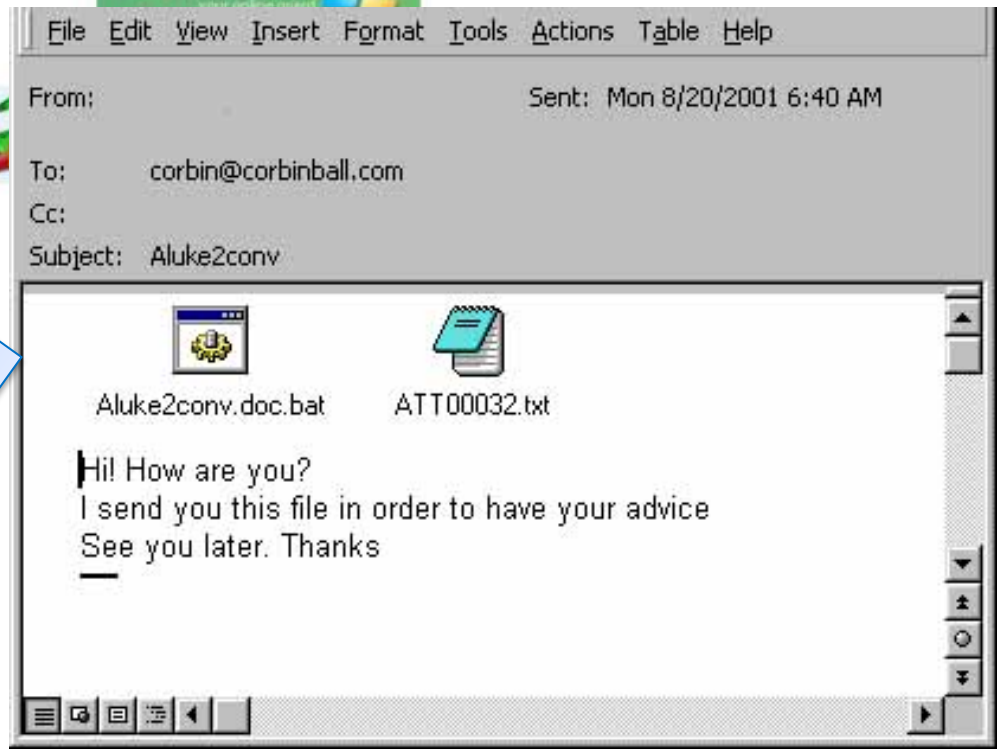


Chain of custody

Other applications…

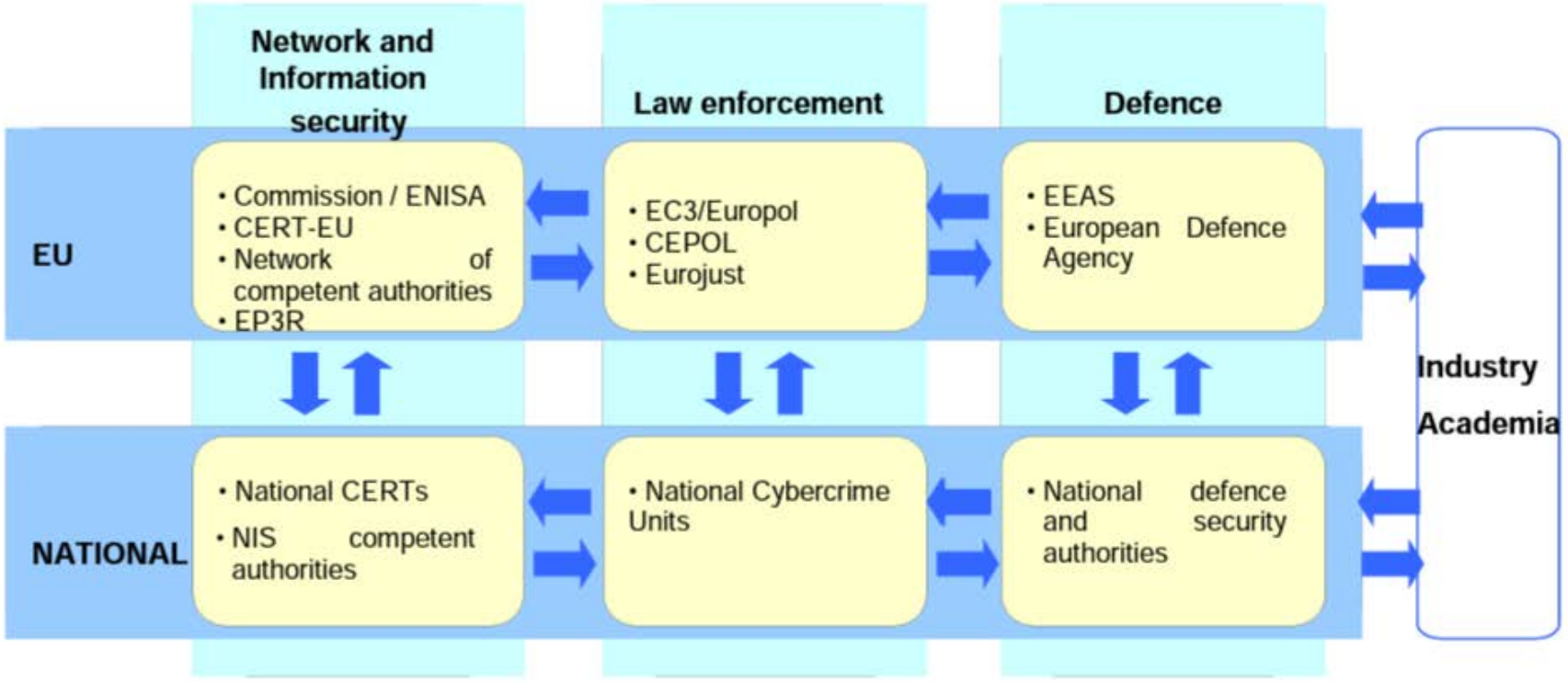


What's the difference?



Microsoft

EU Model


Network and Information security
Law enforcement
Defence
EU
• Commission / ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
Industry
Academia
NATIONAL
• National CERTs
• NIS competent authorities
• National Cybercrime Units
• National defence and security authorities

Cyber-Forensic: Is it possible?

Key points to remember..

- ✓Digital evidence is (real, direct, documentary, etc…) evidence
- ✓Chain of custody is….
- ✓The success of cyber-forensic depends on ….
- ✓CERT is responsible for….
- ✓A forensic process includes the phases…