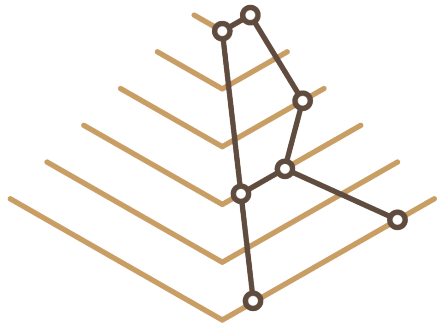
INTERNET FORENSIC PLATFORM FOR TRACKING THE MONEY FLOW OF FINANCIALLY-MOTIVATED MALWARE



RAMSES

Dr. Holger Nitsch
Bavarian University of Policing

Project Fiche

RAMSES

- Topic: **FCT-04-2015 - Forensics topic 4: Internet Forensics to combat organized crime**
- Duration: **36 Months (September 2016– August 2019)**
- Budget:
  - Total: 3 803 087 €
  - Requested: 3 532 000 €
- Consortium:

2 SME's: TREE and TRI

3 public authorities: MJ, BFP, MI

1 research centre: RISSC

5 universities: UNIKENT, UCM, POLIMI, BayFHVR, USAAR

General

- Internet as a key piece of any business activity.
- Criminal activity is not an exception.
- Some crimes previous to the Internet, such as thefts and scams, have found in the Internet the perfect tool for developing their activities.
- The Internet allows criminals hiding their real identity and the possibility to purchase specific tools for stealing sensitive data with a very low investment.
- The overall objective of RAMSES is to design and develop a holistic, intelligent, scalable and modular platform for Law Enforcement Agencies (LEAs) to facilitate digital Forensic Investigations.
- The system will extract, analyze, link and interpret information extracted from Internet related with financially-motivated malware.

CONSORTIUM

RAMSES

COORDINATOR

treelogic

POLICIA JUDICIÁRIA

University of Kent | Computing

RISSC
Centro Ricerche e Studi Su Sicurezza e Criminalità

UNIVERSIDAD COMPLUTENSE MADRID

Fachhochschule für öffentliche Verwaltung und Rechtspflege in Bayern

Trilateral Research & Consulting

POLITECNICO MILANO 1863

Politie Police

CISPA
Center for IT-Security, Privacy and Accountability

CUERPO NACIONAL DE POLICIA

European Commission

Project AIMS

The objective of this project is to design and develop a holistic and intelligent platform for Law Enforcement Agencies to facilitate Forensic Investigations. The system will extract, analyse, link and interpret information extracted from Internet (including Deep Web and Dark net) related with financially-motivated malware. RAMSES project will focus on two use cases: ransomware and banking malware.

- **OBJ.1** - Developing effective guidelines and collaborative methodologies for LEAs investigations
- **OBJ. 2** - Developing a set of tools for Internet Forensics
- **OBJ.3** - Demonstrating the impact of the RAMSES platform, through several pilot exercises in different countries, training and awareness campaigns.

Aims

GOAL 1
Methodology advancement

- LEAs' procedures
- Ethical implications
- Societal impact
- Legal compliance
- Stakeholders engagement
- Guidelines & best practices

GOAL2
RAMSES platform

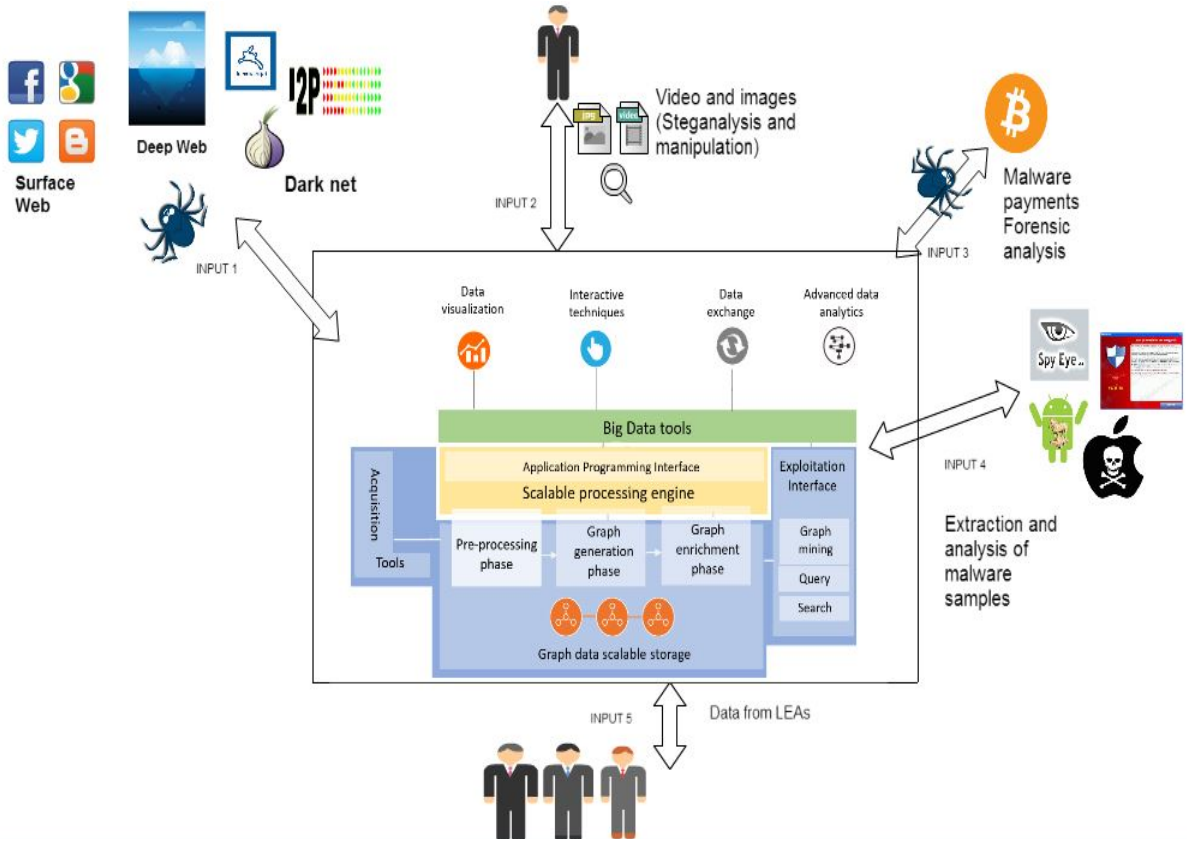
- Data privacy & security
- Advanced analytics
- Predictive engine
- User-oriented tools
- Interoperability

GOAL3
Operational demonstration

- Pilot projects (3 EU countries)
- Impact assessment
- Societal impact evaluation
- LEAs training

RAMSES platform

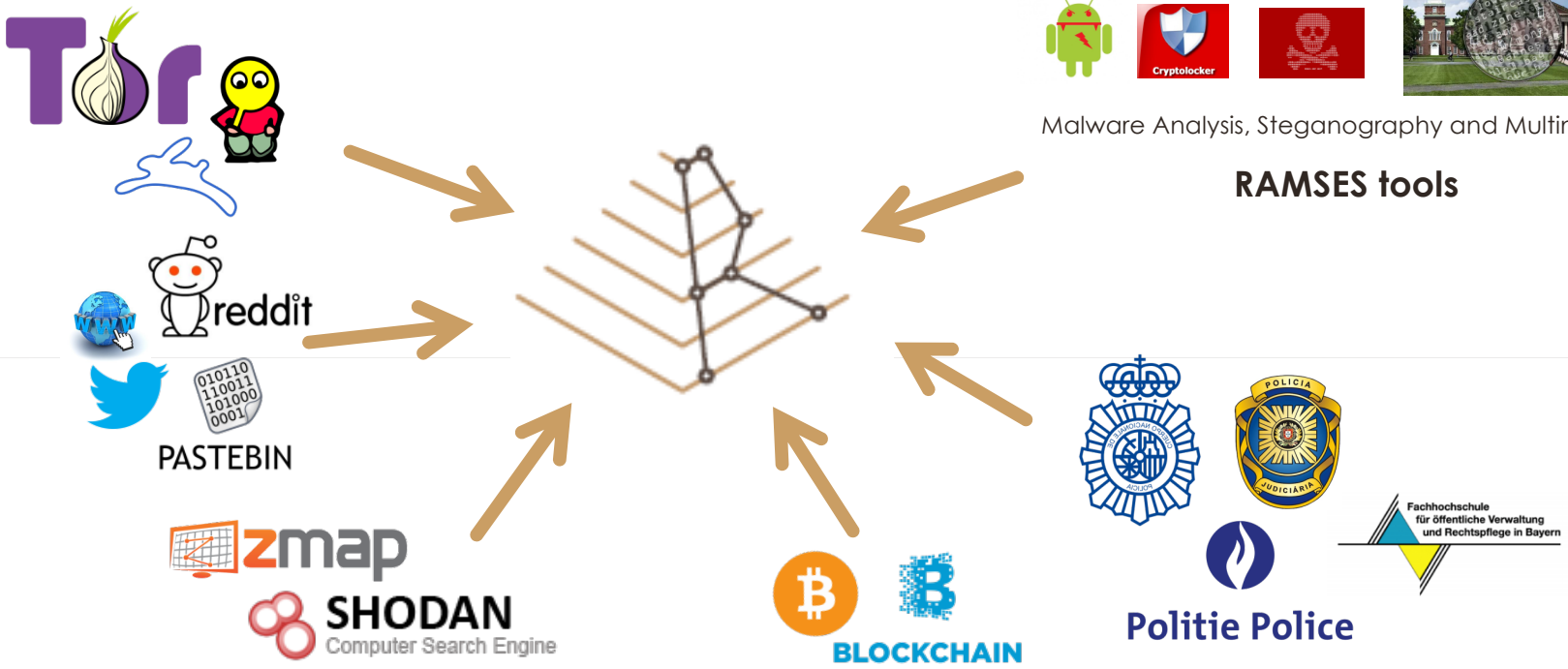
- Module for **automatic extraction of important data related to malware from surface web** (social networks like Facebook, Twitter, forums), Deep Web, and Dark net
- Module for **analysis of malware related payments**
- Module for the **analysis of Images and Videos (manipulation and steganalysis in video and images)**
- Module **to extract and analyse malware samples**
- Module for visualizing the results of the analysis



PLATFORM APPROACH

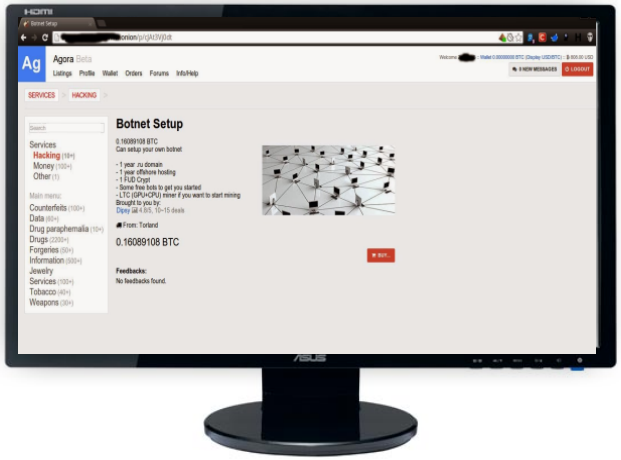
RAMSES

RAMSES Concept:



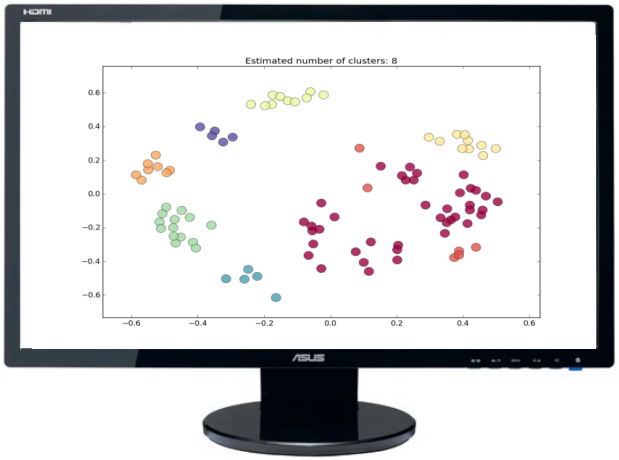
RAMSES Platform: Functionalities

SEARCH



To search **among large** volumes of data already processed. **Search for** an ip, a nickname, a technology, a name of RAT or **any keyword interesting** for the investigator.

Interactive dashboards



To **visualize** the different process of **malware clustering and forensics**. There will be a GUI for visualising the results from machine learning process.

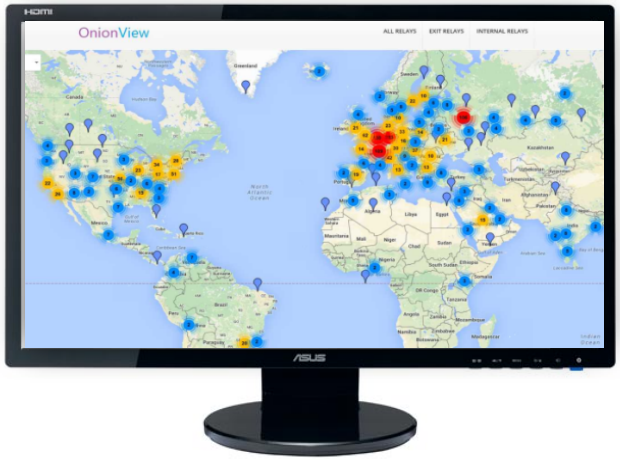
RAMSES Platform: Functionalities

RAMSES

Explore

To **explore the relationships** between different entities **(e.g. ips, usernames, malware name, domains, etc)**

ALERTS

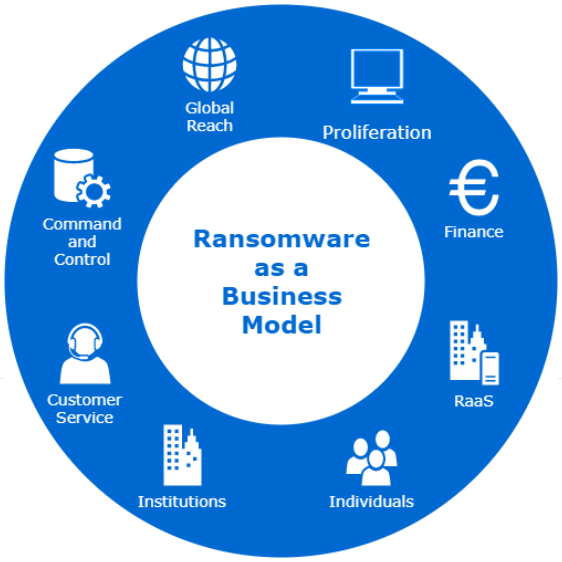


To **show important events** that could be useful for LEAs. For instance, the **deanonymization of a hidden service** selling malware, etc. The **alerts are being defined by LEAs.**

An Economic Model of Ransomware

RAMSES

- Identify how Ransomware makes money
  - Revenue streams
  - Costs
- Predicting how this is likely to evolve
  - Response to competition
  - Response to IT measures (e.g. backups)
- Increasing the cost of Ransomware as a business
  - A better informed/protected public
  - LEAs able to predict future optimisations of Ransomware



European Commission

Spend Money to Take Money

- Ransomware has high fixed costs and very low (zero) marginal costs of attack.
- This should act to choke off competition and encourage ‘efficiency’. How many ransomwares succeed?
- The marketization of services within the ‘ransomware chain’ is a crucial development in the business model.
- This does not reduce fixed costs but it does make it easier for criminals to make a viable ‘business model’.
  - Distribution networks
  - Ransomware as a service
  - Customer service
  - Money laundering
  - Short life before need new product

Setting a Price

- Uniform Pricing is most common
  - Simple, but must be set at an appropriate price
  - We think prices are currently too low
- Price discrimination requires additional information
  - Cooperative malware, and/or specific demographic
  - Look around before encrypt
  - Selective encryption of files
- Bargaining was found to diminish the ransomer's position
  - Being known to negotiate invalidates your initial offering

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

Examples of Ransomware that allow negotiation (F-Secure, 2017)

Simple Game of Ransoming

1. The criminal decides if they will infect the victim's machine
2. Criminal sets ransom demand $D > 0$
3. Victim receives demand and may propose counter offer C
4. The criminal may irrationally destroy files, resulting in a payoff of $-Y < 0$ for the criminal, and $-W < 0$ for the victim
    i. Y represents the cost of time spent by criminal
    ii. W represents the victim's valuation of their files
5. Criminal may release files for C. If $C < M$ (a minimum acceptable offer held secretly by the criminal), the files will be destroyed
6. The criminal may be caught with probability *q*. It is less costly to be caught having not destroyed files.
    i. -X is a reduction of cost –Z for the criminal for potential cooperation with authorities or perceived 'good' behaviour

Outcome	Payoffs	
	Criminal	Victim
Criminal doesn't infect computer	0	0
Release of files for C	C	-C
Files destroyed	-Y	-W
Criminal caught after release of files	-X	0
Criminal caught after destruction of files	-Z	-W

Table 1: Payoffs to different outcomes
Simple games of kidnapping
(Hernandez-Castro, Cartwright, & Stepanova 2017)

Opposed Game of Ransoming

1. Victim chooses how much to spend E on defensive measures
2. Criminal chooses whether to attack
   i. This incurs additional cost A on the victim, representing active countermeasures
3. The attack fails with probability $\theta(E)$
   i. θ is a continuous monotonically increasing function of E
   ii. With probability 1- θ(E) the attack succeeds
   iii. A failed attack costs the criminal –F (effort/resources expended)
   iv. A failed attack costs the victim –A-E (combined cost of defense)
4. If successful, criminal demands C as ransom
   i. Victim can choose whether or not they pay
   ii. If they pay, they regain their files. Criminal gets C and victim pays costs –C and -E
   iii. If they don't pay, their files are destroyed, and they incur costs –W (victim's valuation of files) and -E

Outcome	Payoffs	
	Criminal	Victim
No attack	0	-E
Failed attack	-F	-A-E
Release of files for ransom C	C	-C-E
Ransom not paid	-L	-W-E

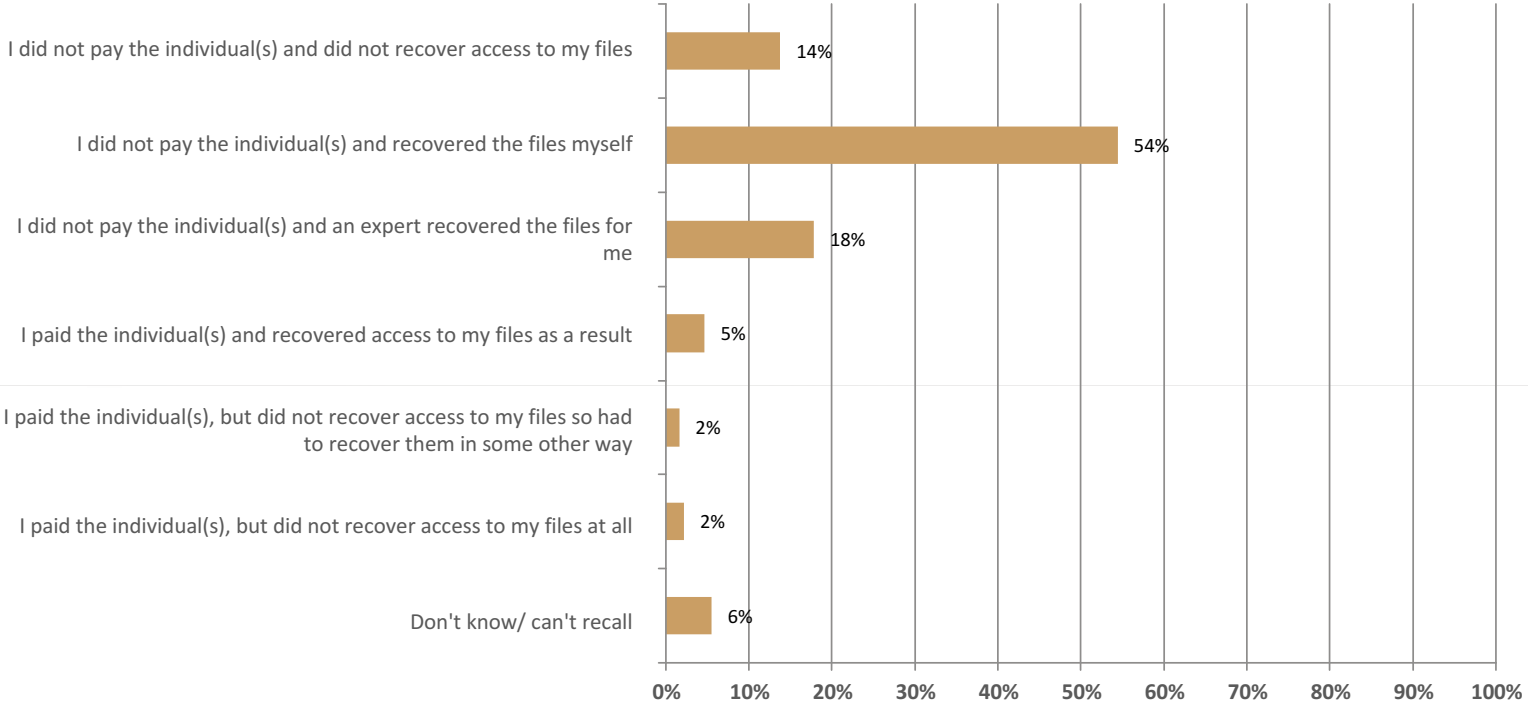
Table 2: Payoffs to different outcomes Kidnapping with possible deterrence (Hernandez-Castro, Cartwright, & Stepanova 2017)

The Victim's Perspective

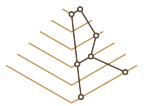
- Willingness to pay isn't just a matter of file value
  - Perception of the situation matters
  - Social engeneering
- The ransom payment must be seen as a calculated risk
  - Reasonable chance of ransom being honoured
  - Files of sufficient worth to ransom
  - The victim must be able to rationalise payment
- Ransomware that provides support for ransom payment is more successful

2 versions of Cryptolocker and the recent Wannacry front-end

Attitudes – ex-post



Competition or infighting



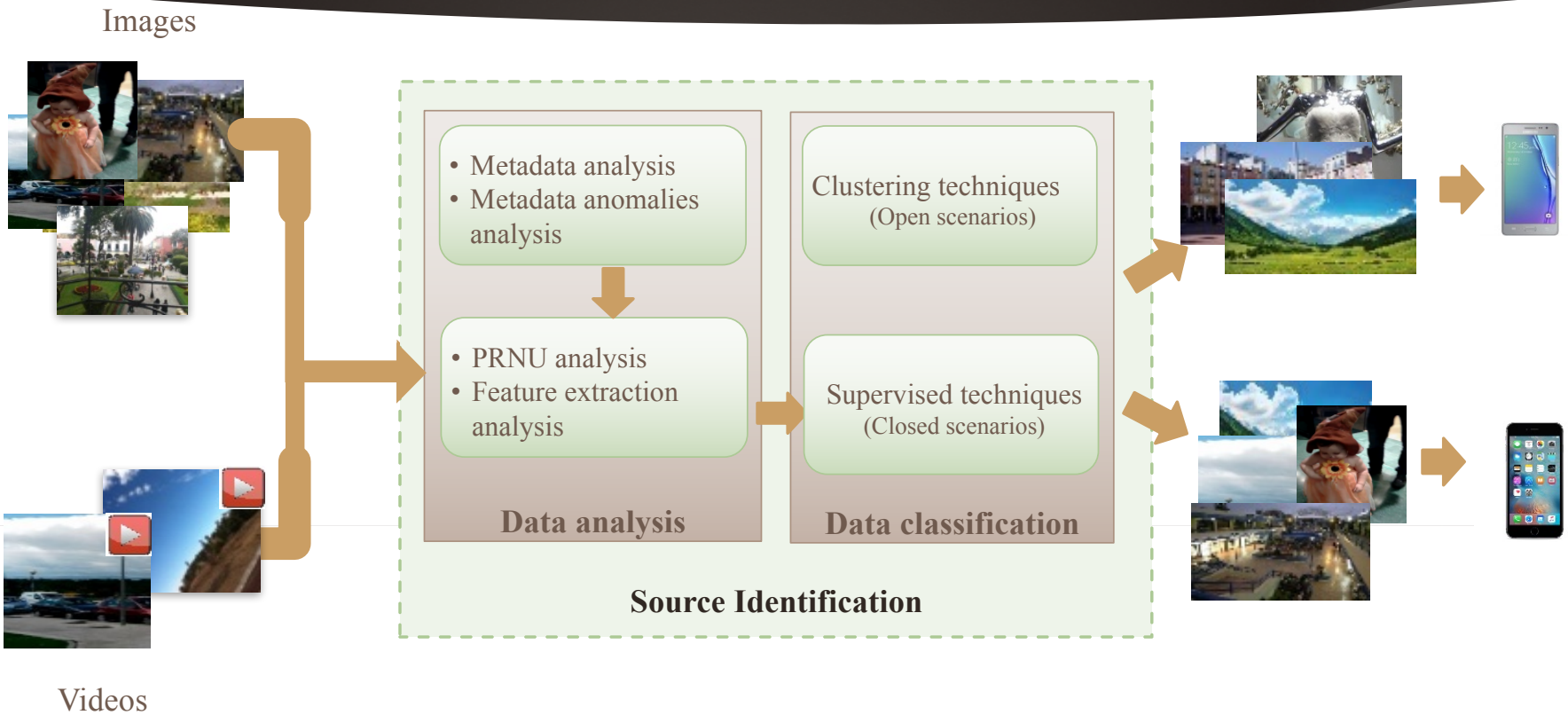
- Ransomware can only succeed as a business model if victims have a good chance of getting their files back.
- The criminals have to offer a **service to customers**.
- Unknowing criminals jumping on the bandwagon or political groups using ransomware as a cover for other attacks undermines the business model. It gives ransomware a **bad reputation**.
- We can expect more sophistication and organization on the criminal side.

Module for analysis of malware related payments

RAMSES

- **Banking Trojans: Prometheus**
  - Memory Forensics for Banking Trojan Detection
  - Analysis and identification of Trojans that modify the web-pages to steal banking credentials
- **Bitcoin Tracker: BitIodine**
  - Automatic extraction of intelligence from the bitcoin network to classify and visualize information
  - Tracking Money Flow

Module for the analysis of Images and videos - Authorship Identification



- As **outputs**, the tool extracts **meta-data** information about the media, the **brand** and the **model** of the device

Steganography

- What is Steganography?
  - The process of hiding information in plain sight.
  - To keep sensitive information hidden and secured against third party attackers.
- Inside the Digital Domain
  - The pervasive nature of digital media content provides a perfect cover for hiding secret messages.

Txt / Image / Audio / Video - Any file or format that contains redundancy.

Steganography

- The pursuit of identifying and proving the existence of steganography
- Simply put, its a decision question. Given any object, does it contain steganography? Or is it clear of secret messages?
- Steganalysis only needs to prove the existence of a secret message. Extracting and reading the message will often involve the efforts of cryptanalysis.

Questions? Comments?

- Thank you!

Dr. Holger Nitsch, holger.nitsch@pol.hfoed.bayern.de,

University of the Bavarian Police