VIRTCRIME

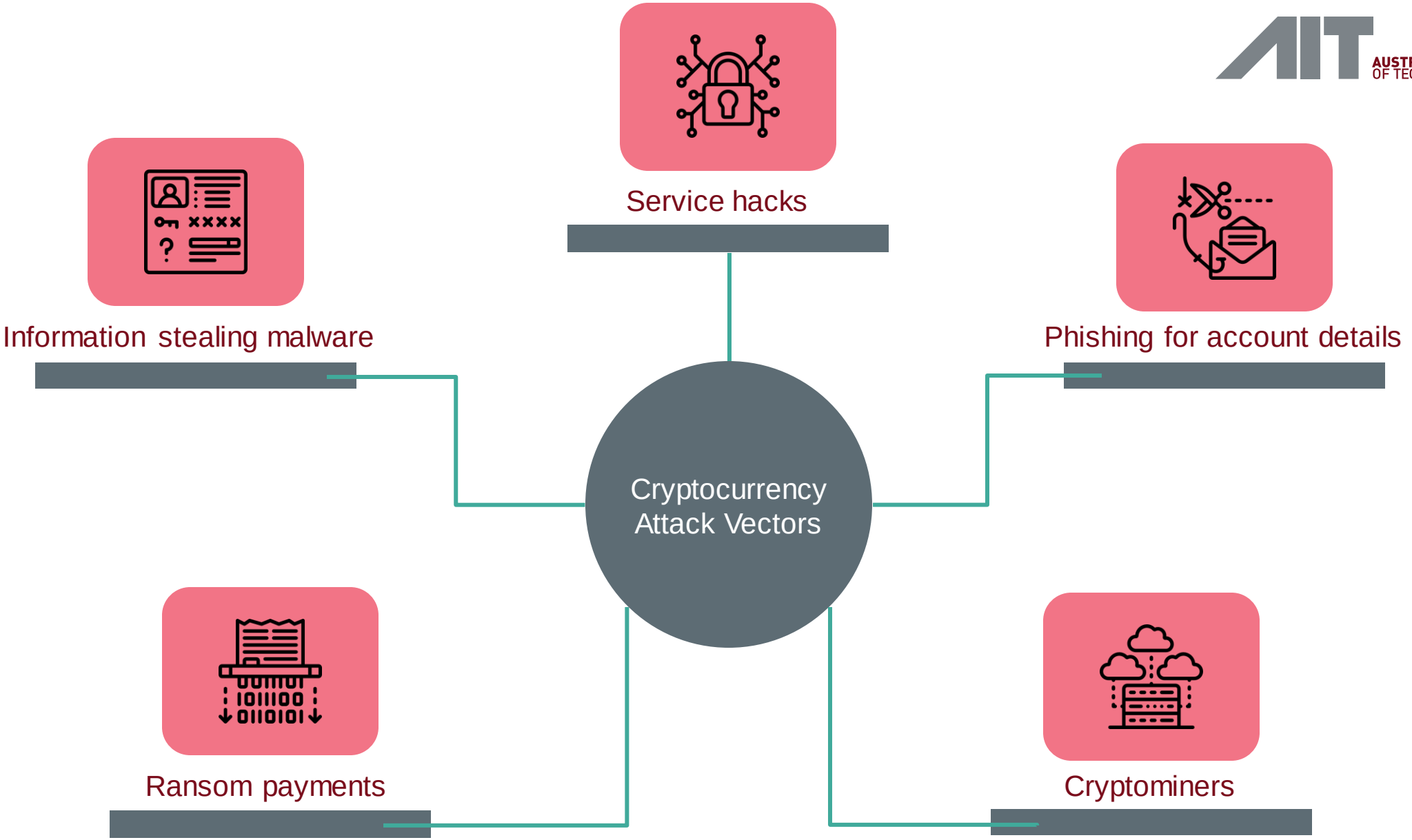
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CRYPTOCURRENCY FORENSICS WITH GRAPHSENSE

VIRTCRIME Training Event

Innsbruck, November 7th 2019

Dr. Bernhard Haslhofer
Senior Scientist
Center for Digital Safety & Security



[Source: EUROPOL Internet Organized Threat Assessment Report 2018]

INSTRUCTIONAL GOAL

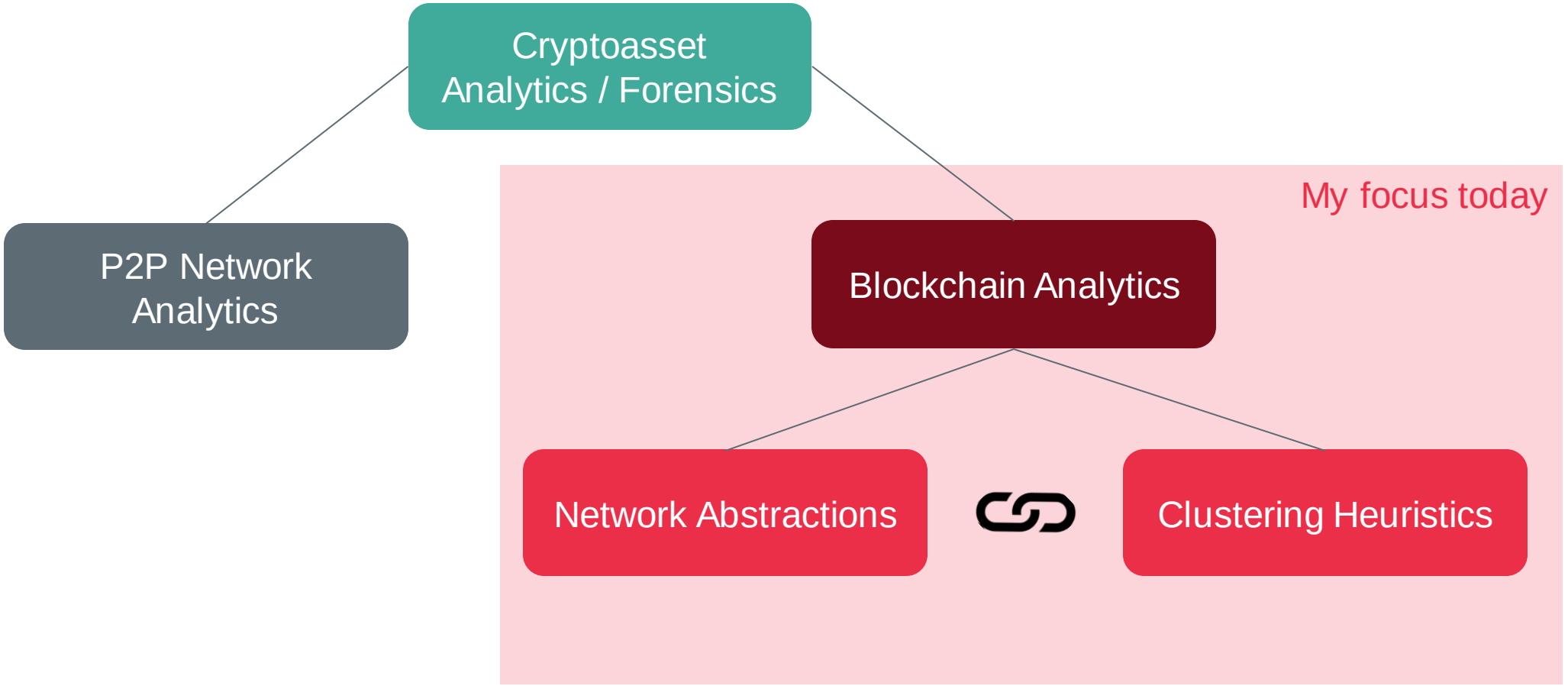
The participants will learn the concepts of the GraphSense cryptocurrency analytics platform and how to use its dashboard to perform basic analytical tasks.

LEARNING OBJECTIVES

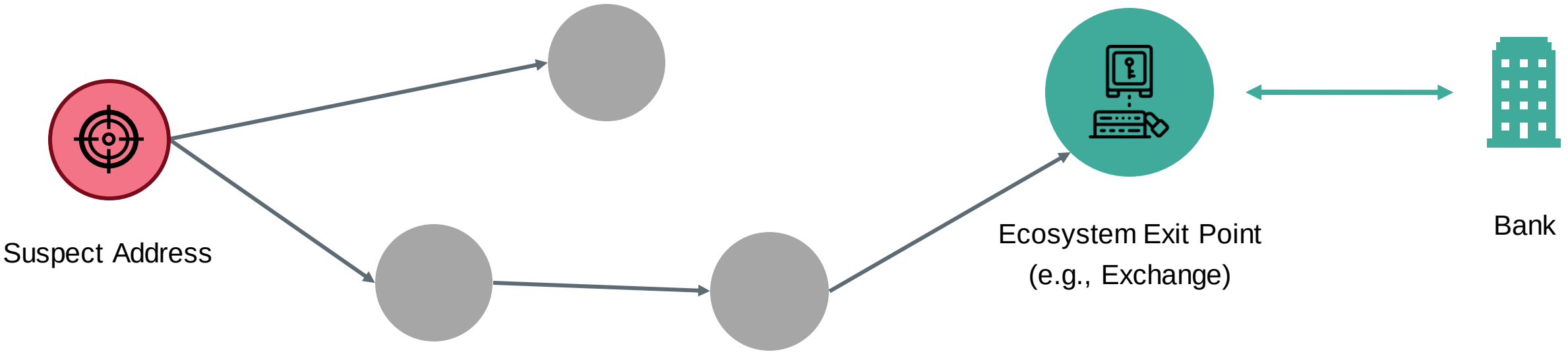
After this block of instructions, the participants will be able to

- Apply the basic cryptocurrency forensic method
- Inspect cryptocurrency addresses and trace monetary flows
- Distinguish between two types of representations: addresses and clusters
- Conduct basic cross-ledger analytics tasks
- Assess the opportunities of data-driven analytics tasks

FORENSIC METHODS | OVERVIEW

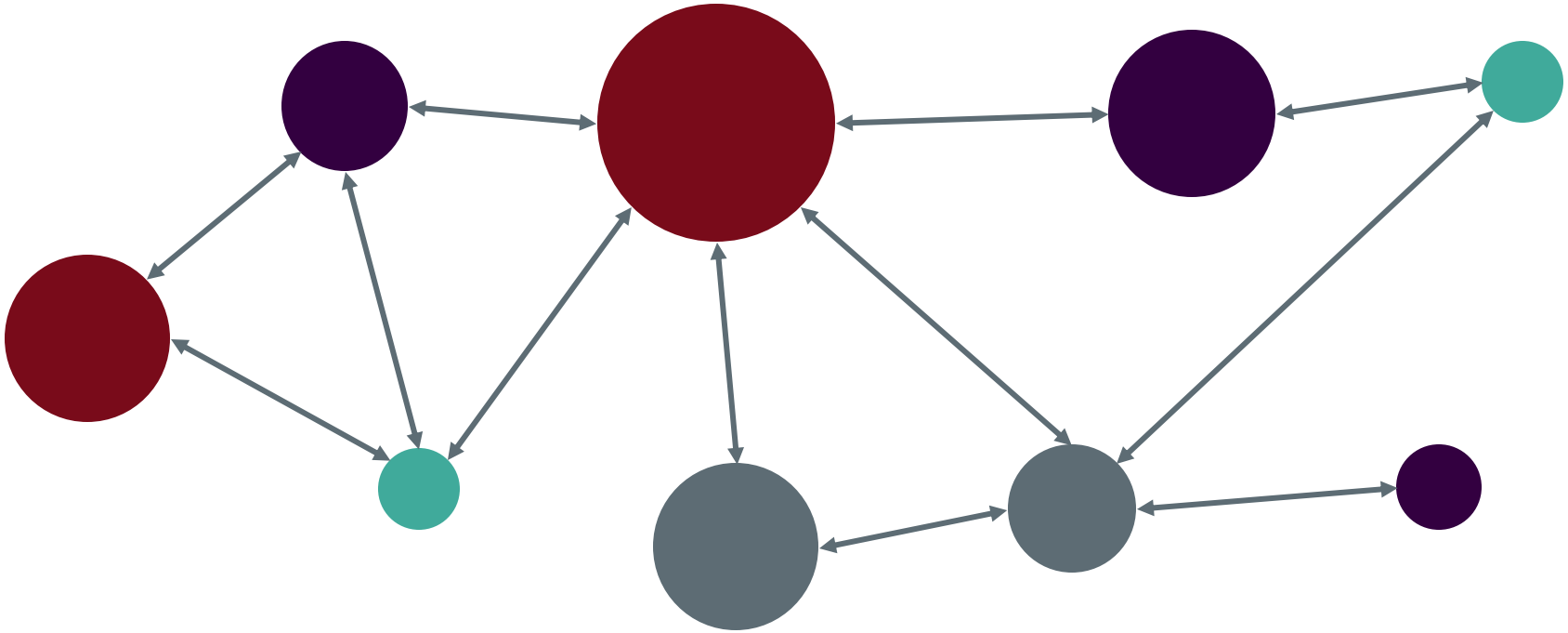


FORENSIC METHODS | BASIC APPROACH



Follow the digital trace of payments
up to a known exit point (typically exchange).

FORENSIC METHODS | NETWORK ABSTRACTION



Nodes: Real-world actors like Exchanges, (Darknet) Marketplaces, Payment Providers, etc.

Edges: Financial transactions between those actors

EXERCISE 1 | INSPECTING ADDRESSES

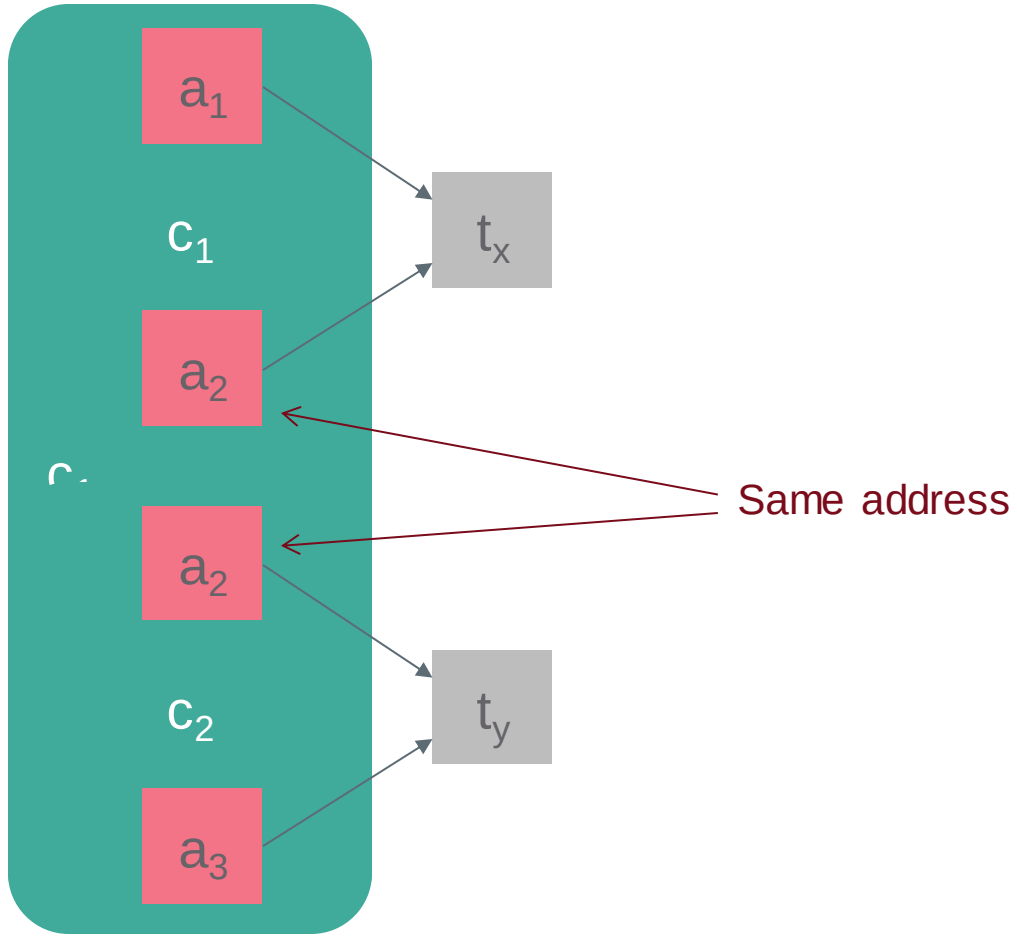
- Open the GraphSense Dashboard: https://beta.graphsense.info
  - Please…no Internet Explorer!
  - Username: graphsense_demo
  - Password: preview

- Search for the BTC address starting with 1BettingE:

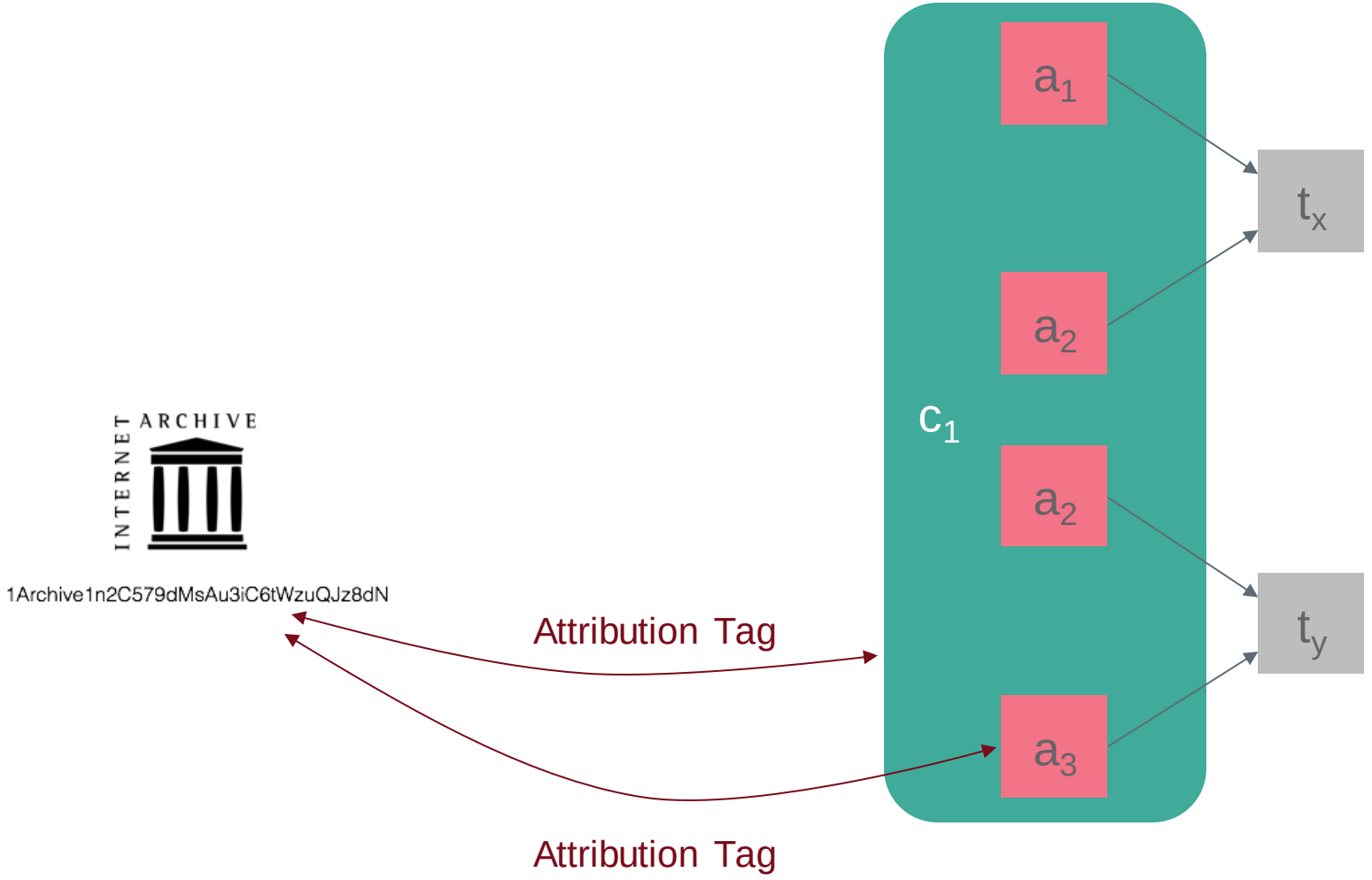
- How much has this addresses received in BTC and EUR?

- In how many transactions has this address been involved?

FORENSIC METHODS | CLUSTERING HEURISTICS



FORENSIC METHODS | CLUSTERING HEURISTICS



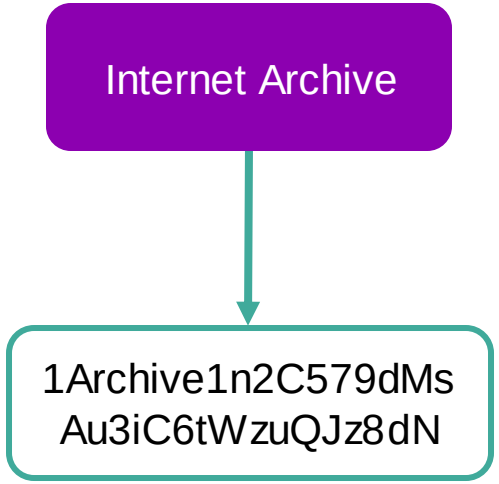
EXERCISE 2 | INSPECTING CLUSTERS

- Make sure 1BettingEynX2Lg24jnmCGDHL3vC6r9yX1 is still your focus node
- How many other addresses are in the same cluster?
- How much has this cluster received in BTC and EUR?
- In how many transactions has this cluster been involved?

ATTRIBUTION TAGS

- Attribution tag = any form of context information that can be attributed to an address (e.g., name of an exchange)

- Challenges
  - Collection, curation and sharing of attribution tags
  - Data protection and privacy laws (e.g., GDPR)
  - Court-proof evidence



ATTRIBUTION TAGS | TAGPACKS

- A collection of attribution tags with associated provenance metadata
- Follow a certain TagPack structure
  - Header (provenance metadata)
  - Body (collection of tags)
- Allows categorization of tags using a configurable taxonomy
- Can be tailored to specific needs

Title: Demo TagPack
Creator: Bernhard Haslhofer
Description: For demo purposes
Lastmod: 2019-03-15
Source: https://archive.org/donate/cryptocurrency
Category: Organization

address: 1Archive1n2C579dMsAu3iC6tWzuQJz8dN
currency: BTC

...

address: t1ZmpK4QFcvyQZ3ghTgSboBW8b4HgiZHQF9
currency: LTC

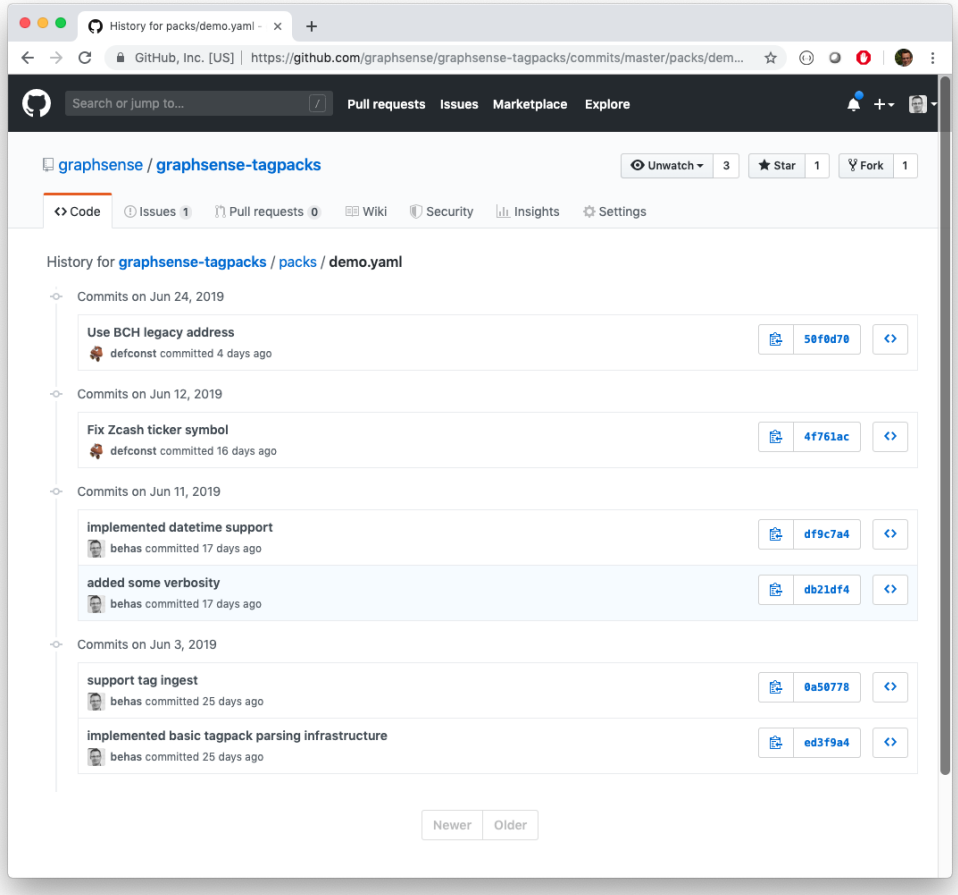
https://github.com/graphsense/graphsense-tagpacks/blob/master/packs/demo.yaml

ATTRIBUTION TAGS | COLLABORATIVE SHARING

- TagPacks should remain simple
  - minimal number of fields
  - avoid semantic ambiguities

- However, full data provenance requires more, e.g., who added/modified/deleted what and why?

- Idea: use Git
  - Standard tool in SW development
  - Provides most of the features we need



ATTRIBUTION TAGS | LEGAL REQUIREMENTS

- Must have a legal basis and comply with data protection principles
- Verifiability: procedures must be repeatable and reproducible; tags must remain available
- Chain of evidence: exact information on forensic investigations and traces must be provided
- ….

Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations

Michael Fröwis[a], Thilo Gottschalk[b], Bernhard Haslhofer[c], Christian Rückert[d] and Paulina Pesch[b]

[a] University of Innsbruck, Technikerstr. 21a, 6020 Innsbruck, Austria
[b] Karlsruhe Institute of Technology, Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe, Germany
[c] Austrian Institute of Technology, Giefinggasse 2, 1210 Wien, Austria
[d] Friedrich-Alexander University of Erlangen-Nuremberg, Schillerstraße 1, 91054 Erlangen, Germany

ARTICLE INFO

Keywords:
digital forensics
cryptocurrencies
digital evidence
safeguards
legal

ABSTRACT

Analyzing cryptocurrency payment flows has become a key forensic method in law enforcement and is nowadays used to investigate a wide spectrum of criminal activities. However, despite its widespread adoption, the evidential value of obtained findings in court is still largely unclear. In this paper, we focus on the key ingredients of modern cryptocurrency analytic techniques, which are clustering heuristics and attribution tags. By empirically quantifying the effect of CoinJoin transactions, we illustrate that clustering heuristics can lead to false interpretations. We then discuss clustering heuristics and attribution tags in the light of internationally accepted legal standards and rules for substantiating suspicions and providing evidence in court. From that we derive a set of legal key requirements and translate them into a data sharing framework that builds on existing legal and technical standards. Integrating that framework in modern cryptocurrency analytics tools could allow more efficient and effective investigations, while safeguarding their evidential value.

https://arxiv.org/abs/1906.12221

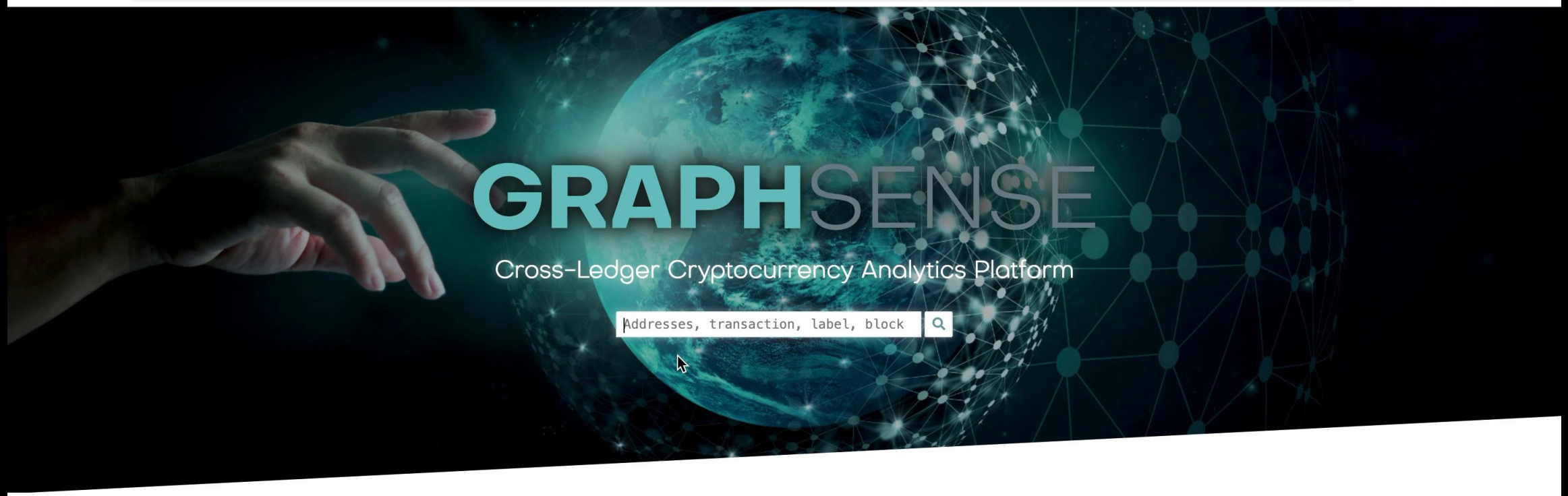
EXERCISE 3 | ATTRIBUTION TAGS

- Wipe the dashboard (new document symbol)
- Search for “Locky” (a well-known ransomware attack)
- How many addresses are tagged as Locky?
- Select an attribution tag and explain its provenance

EXERCISE 4 | AUTOMATED TRACING

- Make sure you still have an address related to locky on the dashboard

- Use the search function (depth: 2) to find an exchange that received money from the Locky attack



Supported currencies

Bitcoin

Last update	10/27/2019 11:56 PM
Latest block	601305
Transactions	469,116,063
Addresses	571,791,497
Entities	275,796,044
Tags	5,783

Bitcoin Cash

Last update	10/16/2019 1:37 AM
Latest block	604736
Transactions	279,880,099
Addresses	303,612,701
Entities	143,656,226
Tags	9

Litecoin

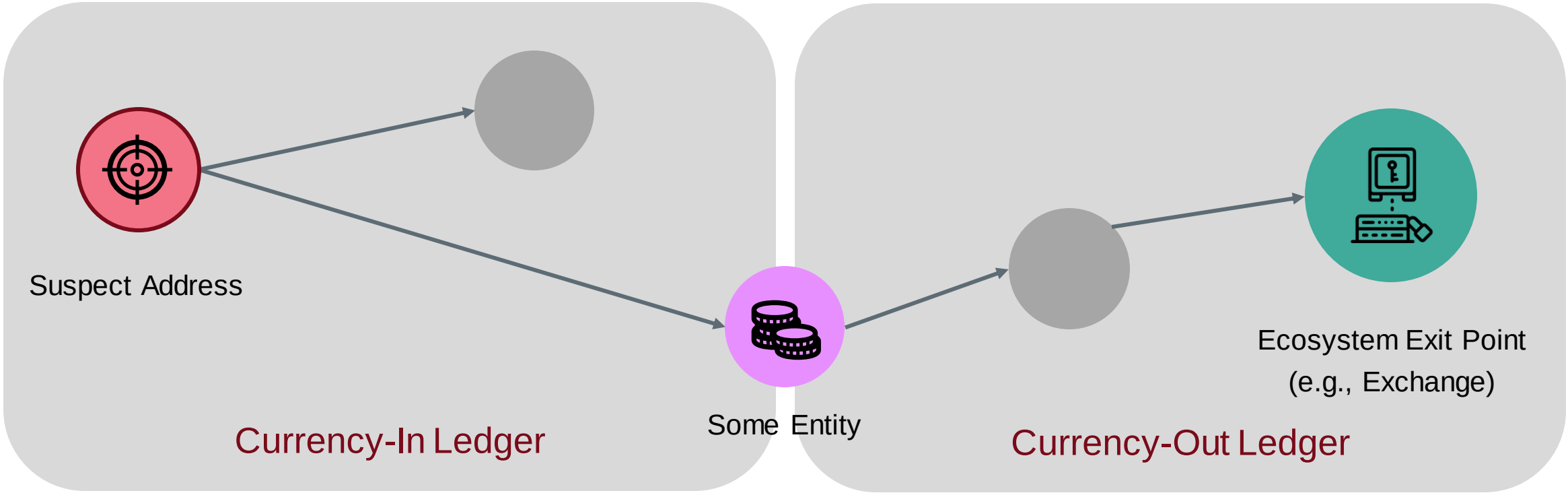
Last update	10/16/2019 1:58 AM
Latest block	1720082
Transactions	38,094,915
Addresses	47,001,625
Entities	24,838,565
Tags	8

Zcash

Last update	10/16/2019 1:57 AM
Latest block	620972
Transactions	5,411,897
Addresses	3,792,433
Entities	1,766,878
Tags	8

GraphSense is supported by the TITANIUM project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740558, and by the VIRTCRIME project, which is funded by the Austrian security research programme KIRAS of the Federal Ministry for Transport, Innovation and Technology BMVIT.

FUTURE DIRECTIONS | CROSS-LEDGER



Needed forensic method: follow the digital trace of payments up to a known exit point (typically exchange) across ledgers

EXERCISE 5 | CROSS-LEDGER ANALYTICS

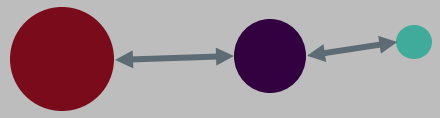
- Wipe the dashboard (new document symbol)
- Search for “Internet Archive” (a non-profit organization in SF)
- Identify a Bitcoin (BTC) and a Bitcoin Cash (BCH) address and place them on the dashboard
- How much has the Internet Archive received in each currency?

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

GOING BEYOND BASIC ANALYTICS TASKS

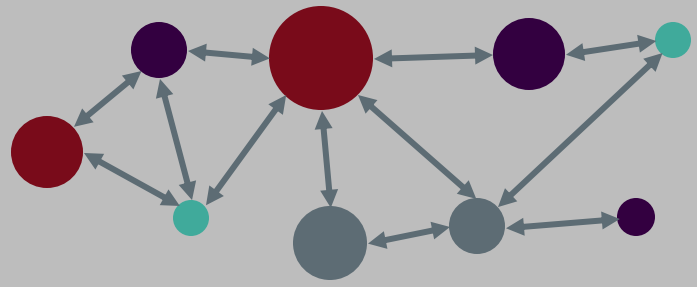
…by writing dedicated analytics jobs and executing them over the entire dataset

INSIGHTS | METHODS



Microscopic Analysis

Useful for following the digital trace of payments



Macroscopic Analysis

Useful for understanding (parts of) an entire cryptocurrency ecosystem

INSIGHTS | RANSOMWARE MARKET

Ransomware Payments in the Bitcoin Ecosystem

Masarah Paquet-Clouston
GoSecure Research
Montreal, Canada
mcpc@gosecure.ca

Bernhard Haslhofer
Austrian Institute of Technology
Vienna, Austria
bernhard.haslhofer@ait.ac.at

Benoit Dupont
Université de Montréal
Montreal, Canada
benoit.dupont@umontreal.ca

ABSTRACT

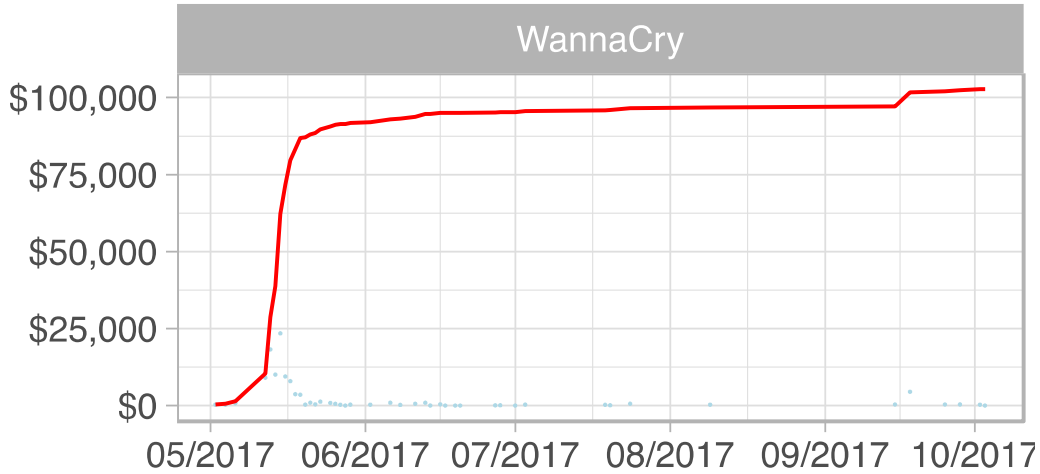
Ransomware can prevent a user from accessing a device and its files until a ransom is paid to the attacker, most frequently in Bitcoin. With over 500 known ransomware families, it has become one of the dominant cybercrime threats for law enforcement, security professionals and the public. However, a more comprehensive, evidence-based picture on the global direct financial impact of ransomware attacks is still missing. In this paper, we present a data-driven method for identifying and gathering information on Bitcoin transactions related to illicit activity based on footprints left on the public Bitcoin blockchain. We implement this method

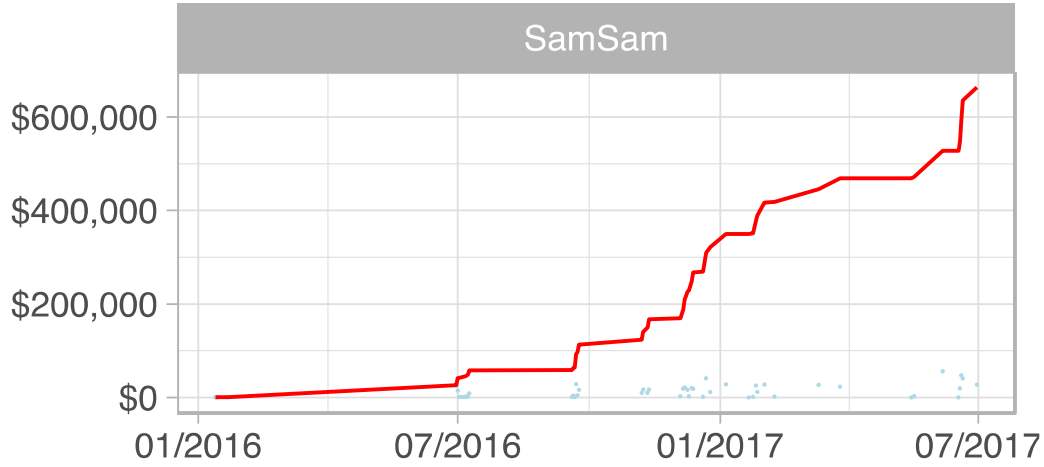
the time of writing, there are 505[1] known ransomware families detected and almost all of them demand payments in Bitcoin [27], which is the most prominent cryptocurrency.

Yet, global and reliable statistics on the impact of cybercrime in general, and ransomware in particular, are missing, causing a large misunderstanding regarding the severity of the threat and the extent to which it fuels a large illicit business. Most of the statistics available on cybercrime and ransomware are produced by private corporations (cf. [29, 38, 39]) that do not disclose their underlying methodologies and have incentives to over- or under-report them since they sell cybersecurity products and services

[Source: https://arxiv.org/abs/1804.04080]

INSIGHTS | RANSOMWARE MARKET





[Source: https://arxiv.org/abs/1804.04080]

INSIGHTS | RANSOMWARE MARKET

Ransomware is a highly skewed market

	Family	Addresses	BTC	USD
1	Locky	6,827	15,399.01	7,834,737
2	CryptXXX	1,304	3,339.68	1,878,696
3	DMALockerv3	147	1,505.78	1,500,630
4	SamSam	41	632.01	599,687
5	CryptoLocker	944	1,511.71	519,991
6	GlobeImposter	1	96.94	116,014
7	WannaCry	6	55.34	102,703
8	CryptoTorLocker2015	94	246.32	67,221
9	APT	2	36.07	31,971
10	NoobCrypt	17	54.34	25,080
11	Globe	49	33.03	24,319
12	Globev3	18	14.34	16,008
13	EDA2	23	7.1	15,111
14	NotPetya	1	4.39	11,458
15	Razy	1	10.75	8,073

Table 4: Received payments per ransom family (Top 15).

[Source: https://arxiv.org/abs/1804.04080]

INSIGHTS | SEXTORTION SPAM

Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem

Masarah Paquet-Clouston
GoSecure
mcpc@gosecure.net

Matteo Romiti
Austrian Institute of Technology
Matteo.Romiti@ait.ac.at

Bernhard Haslhofer
Austrian Institute of Technology
Bernhard.Haslhofer@ait.ac.at

Thomas Charvat
Excello
tc@excello.cz

ABSTRACT

In the past year, a new spamming scheme has emerged: sexual extortion messages requiring payments in the cryptocurrency Bitcoin, also known as *sextortion*. This scheme represents a first integration of the use of cryptocurrencies by members of the spamming industry. Using a dataset of 4,340,736 sextortion spams, this research aims at understanding such new amalgamation by uncovering spammers' operations. To do so, a simple, yet effective method for projecting

Since 2018, sextortion spams have been distributed in a dozen languages, most likely with the use of the Necurs botnet [13, 32]. Shultz [32] already conducted a primary analysis of the sextortion spammers potential revenues by inspecting 58,611 Bitcoin addresses found in two sextortion-related spam campaigns lasting 60 days. He concluded that a total of 83 addresses received approximately $146,280. However, the author only summed incoming payments without applying more advanced methods for tracing monetary flows in the Bitcoin transaction graph, which have already been

[Source: https://arxiv.org/abs/1908.01051]

INSIGHTS | SEXTORTION SPAM

I know *** one of your pass word.

I installed a trojan from the adult videos site

I will send your video recording to your contacts

solution should be to compensate me $1000

via Bitcoin (google "how to buy bitcoin").

BTC Address: 1GYfPNat1uQzrBBKTzftMtZ5TgzNdNmTL9

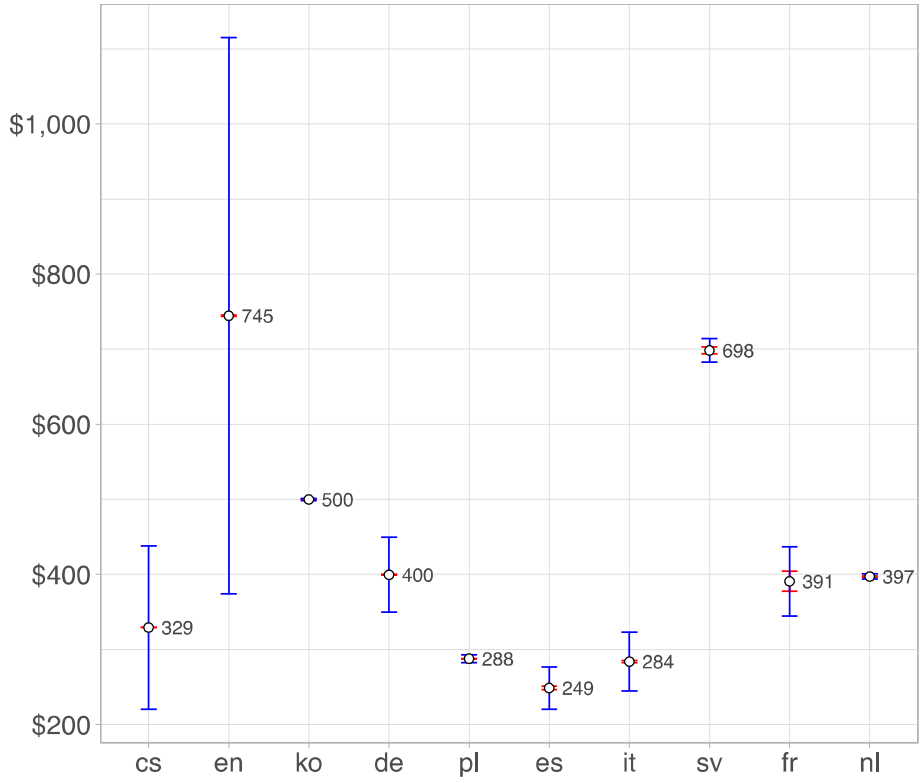
[...]

FAKE!!

[Source: https://arxiv.org/abs/1908.01051]

INSIGHTS | SEXTORTION SPAM

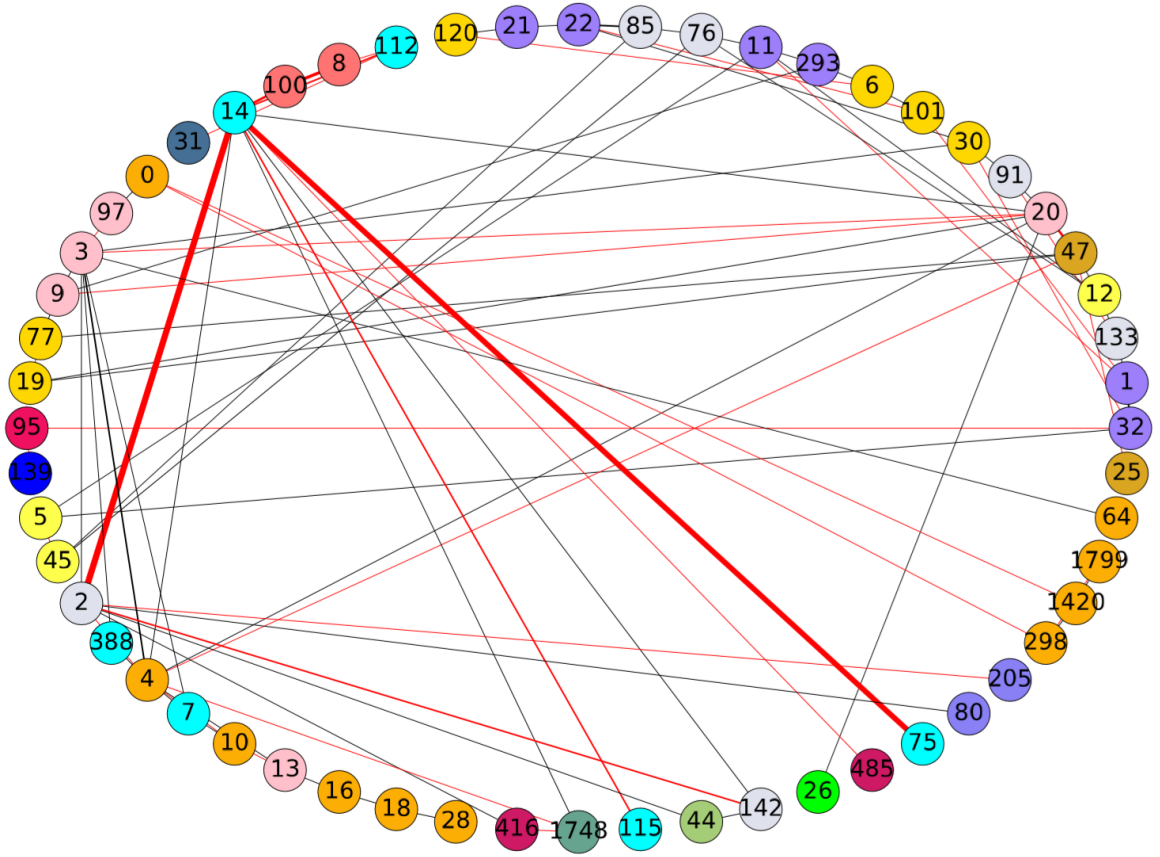
Spammers consider language in their pricing strategy



[Source: https://arxiv.org/abs/1908.01051]

INSIGHTS | SEXTORTION SPAM

There are financial connections among the entities receiving extortion rewards



[Source: https://arxiv.org/abs/1908.01051]

titanium-project.info

virtcrime-project.info

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

bernhard.haslhofer@ait.ac.at

https://graphsense.info

KIRAS Sicherheitsforschung

FFG Promoting Innovation