



22 APRIL 2020

Key DarkNet Investigation Techniques Webinar



JÖRN WEBER

Jörn Weber is an investigator and the managing director of the corma GmbH.

Before his time at corma, he worked as a police officer in NRW for nearly 20 years and left the service as Kriminalhauptkommissar (Detective Chief Inspector).

mail@corma.de



ANASTASIA KORNILOVA

Sales Director
at Social Links

sales@mtg-bi.com

Key DarkNet Investigation Techniques



AGENDA

Maltego Classic / XL and Social
Links Pro features will be
presented

1. Introduction about Social Links

Case 1: Discovering Socials and checking
also Dark Net.

Case 2: Best practice from Jorn for
analysing Dark Net posts.

Case 3: Starting with PGP and checking
what else is there?

Case 4: overview of what can be found
with Social Links in Dark Net.

5. Q & A session

Key facts about Social Links



SOCIAL LINKS



Since 2015, 5 Years of Open Source
Data Mining Tool Development



40+
Sources

700+
Transforms

9TB
Our own Social
Links database



50% EU Law Enforcement organizations
already use Social Links for Open Source,
Social Media and Dark Web Intelligence



Clients from all
around the World
from **55+** countries



TOP 5 Industries: Law Enforcement, Cyber Security, Finance
and Banking, Consulting and Due Dill

Q & A session



ANASTASIA KORNILOVA

SOCIAL LINKS DEMO, TRIAL,
PURCHASE INQUIRIES

sales@mtg-bi.com

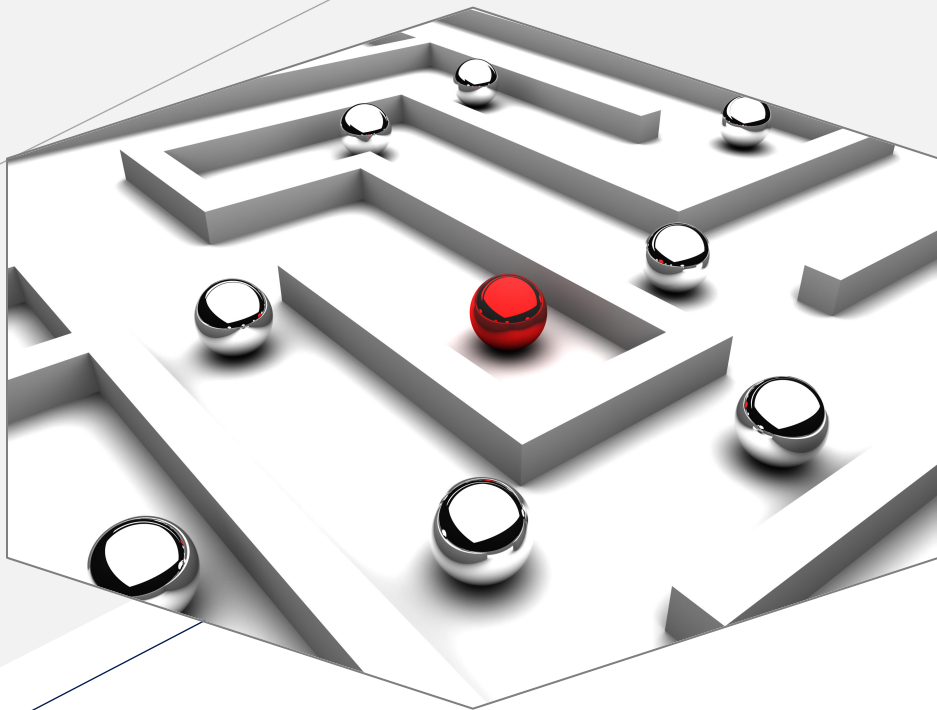


JÖRN WEBER

TRAINING OF MALTEGO AND SOCIAL
LINKS

Register at **corma.training** to get
a **10% discount!**

mail@corma.de



Social Links Webinar: Dark Net Investigations

About us— corma GmbH

Agency for investigations, research and intelligence solutions

- Global Corporate Investigations
- Intelligence Solutions
- Trainings & Workshops
- Based in Germany

About Me: Jörn Weber

Never wonder, always know!

- 19 Years Police Germany (NRW),
Kriminalhauptkommissar a.D.
- since 1999 managing partner **corma GmbH**
- Investigator
- Trainer for:
 - Internet Investigations / OSINT
 - Maltego
 - Social Links
 - Paliscope



Pre-Announcement

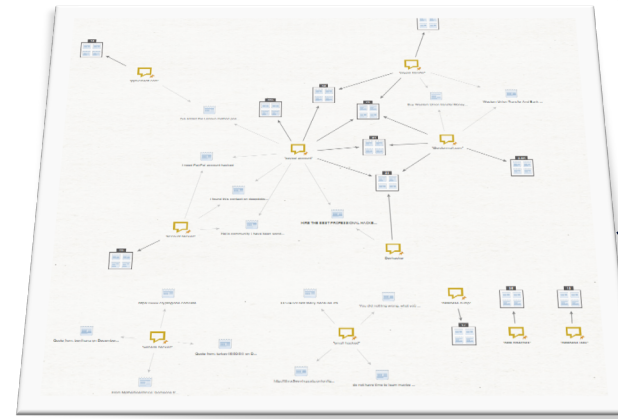
- The first **Maltego Online Video Training** will start soon!
- **Maltego Classic Bootcamp** – German Version – will start on 27th April
- **Maltego Classic Bootcamp** – English Version – will start ~ 5th May
- **Social Links Online Course** – currently beeing recorded

Register at corma.training to get a **10% discount!**



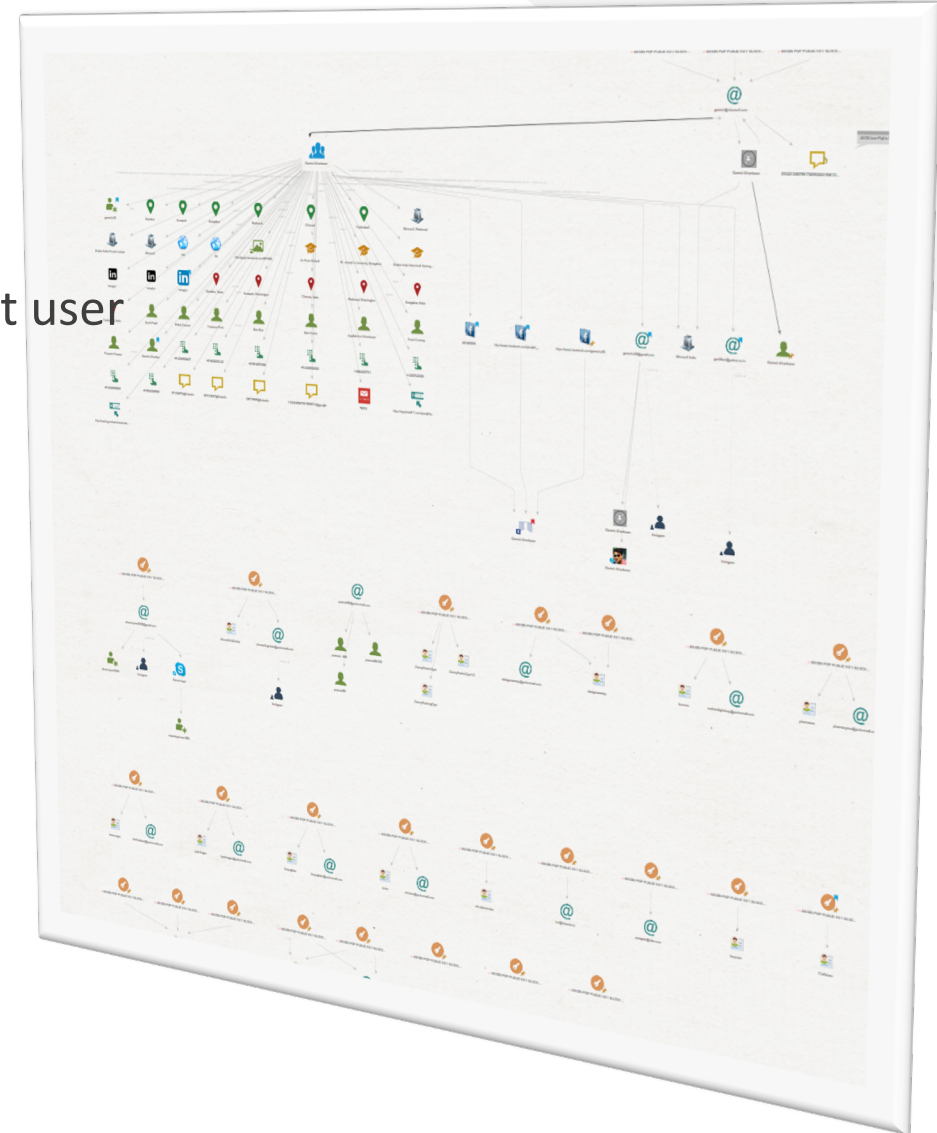
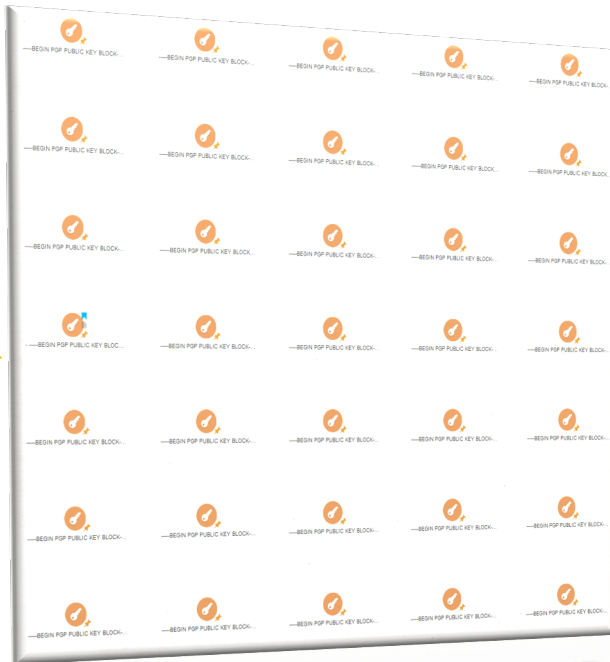
Case 2

- Search for Keyphrases in the Dark Net
- Find the information inside the posts
 - with Maltego
 - with exported data
- Tips:
 - Use „quotation marks“ to avoid unwanted noise
 - create multiple „Phrase Entities“ with different keyword variations -> this allows to see links
 - Select Entity Type „forum post“ and export to table for efficient review outside of Maltego.
 - see instructions at the end of the slide deck



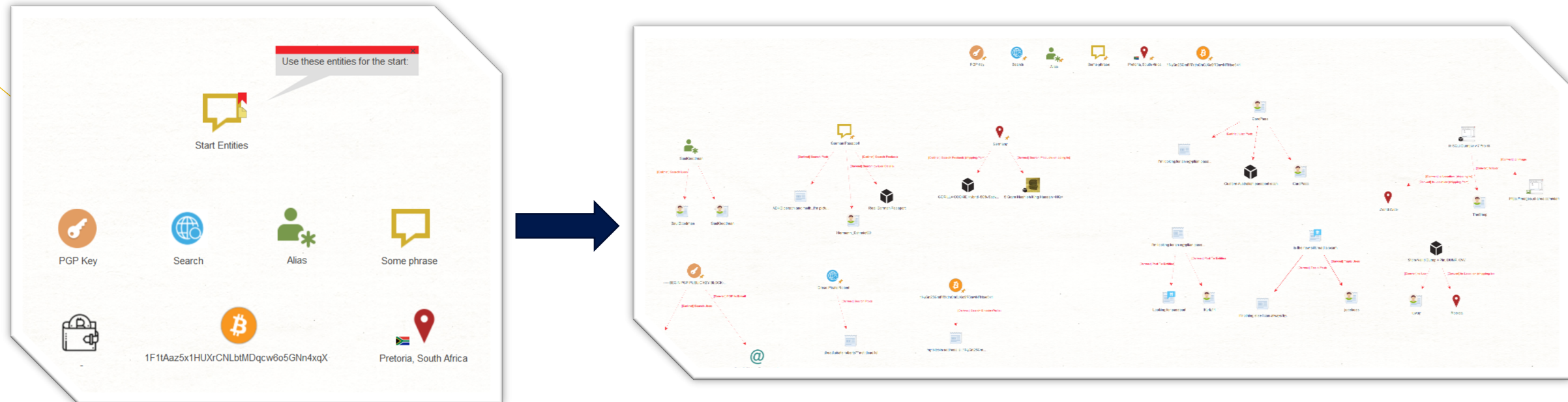
Case 3

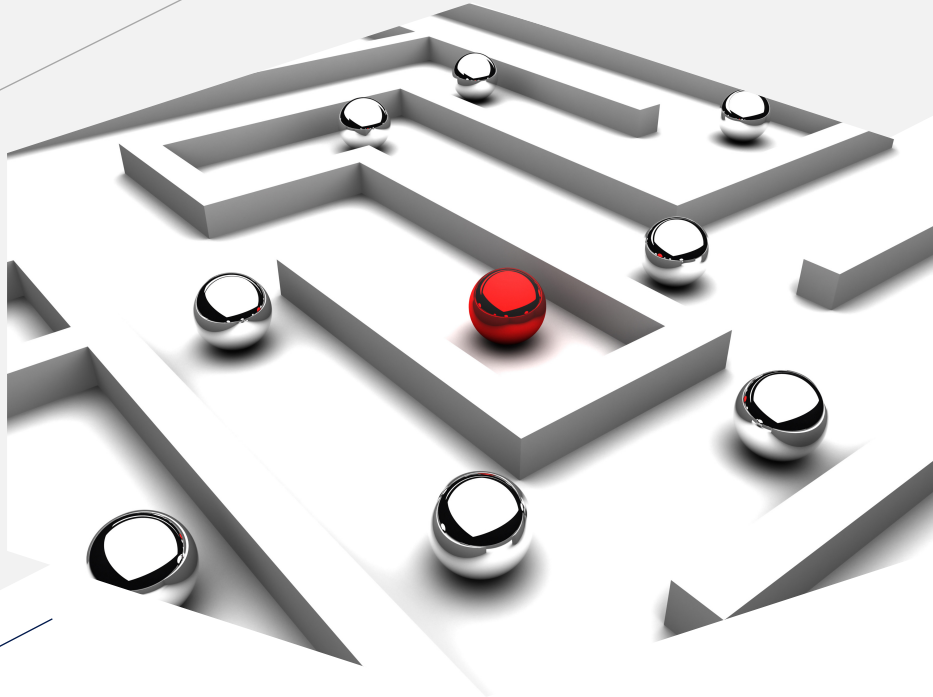
- How to follow links from PGP Keys
- Find the information „within“ public PGP Keys
 - Conduct further investigations into possible Dark Net user
 - Identify the user and related new information
 - Follow the lead



Case 4

- Why should you always use the Social Links Dark Net Transforms?
 - Because it's easy and fast – you never know if that opens a new path to new information.
- Which entities you can (should) use?
- How are they linked?





Thank You



Jörn Weber



+49 2163 349 0081



jw@corma.de



www.corma.de



Twitter: [@corma_agency](https://twitter.com/corma_agency)

corma GmbH
Hochstr. 2
41379 Brüggen
Germany

Online Training Courses: <https://corma.training>
Workshops: <https://corma.de/en>
Blog: <https://corma.de/en/blog/>

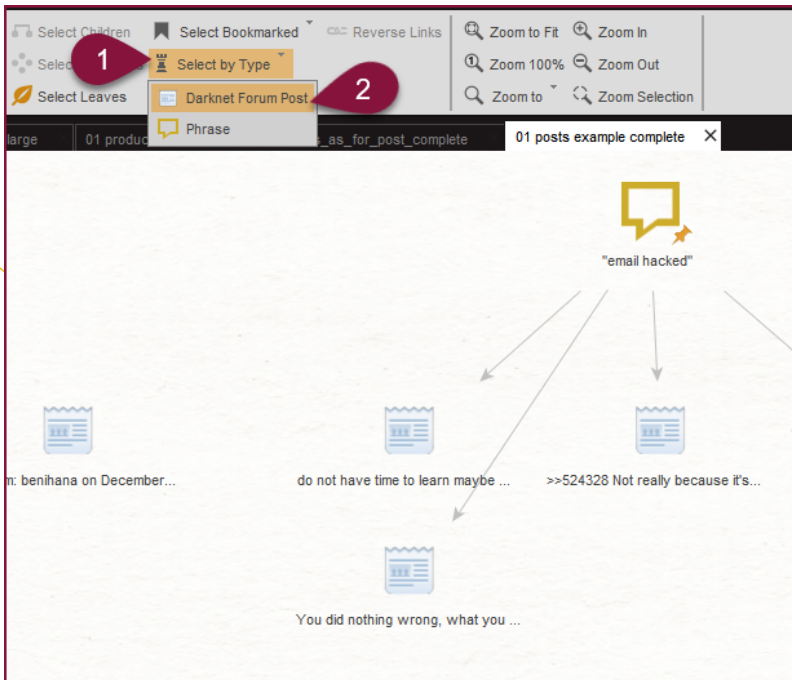


Instructions for Export

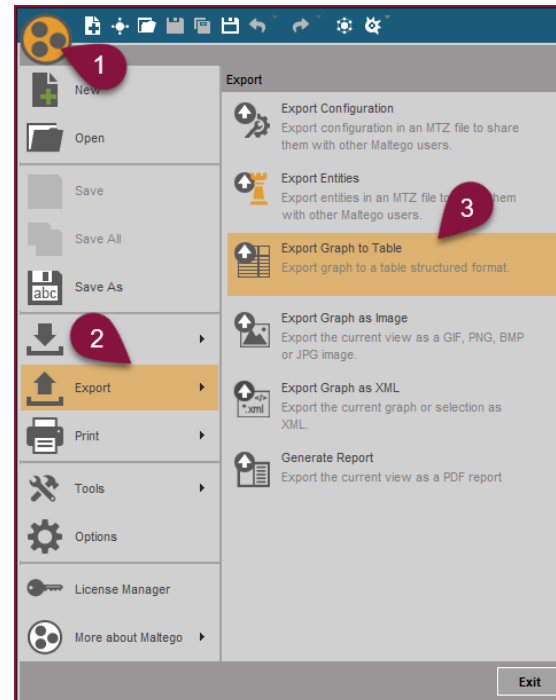
Export Information

Example: Social Links „Dark Net Transforms“

Select „Post“ Entities



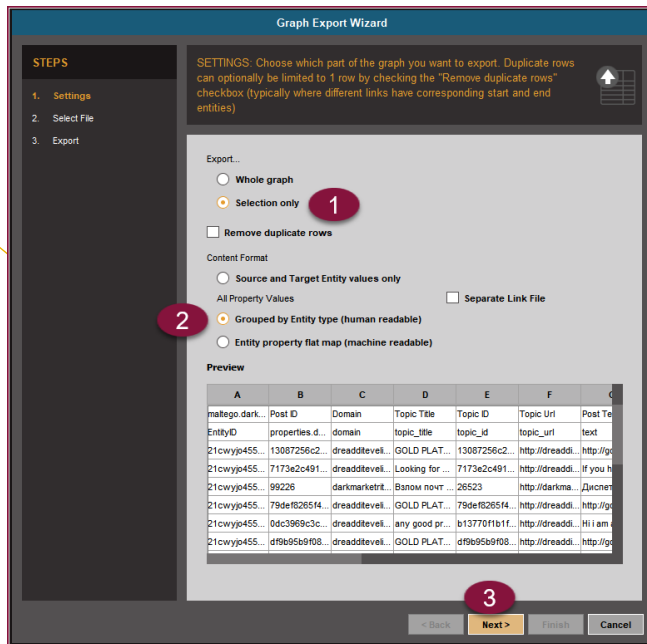
Select „Export Graph to Table“



Export Information

Example: Social Links „Dark Net Transforms“

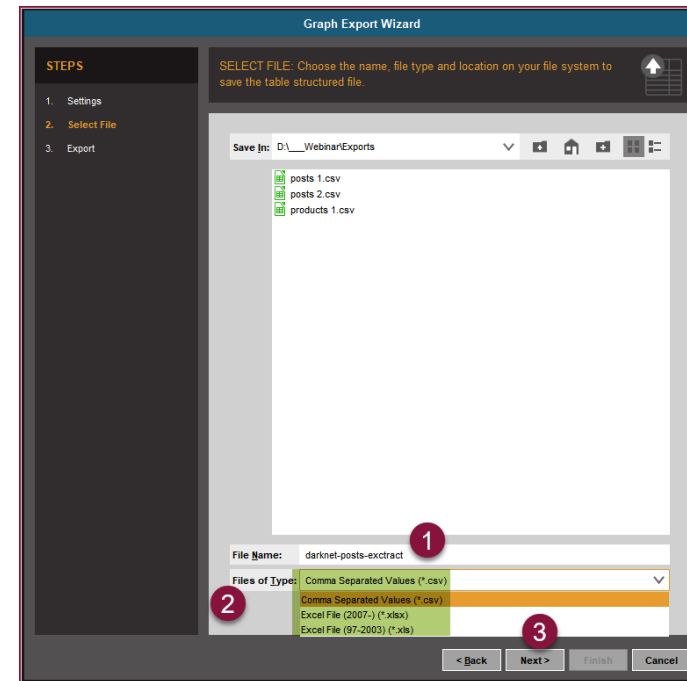
Selection only – human readable



The screenshot shows the 'Graph Export Wizard' interface. The 'STEPS' sidebar on the left indicates the current step is 'Settings'. The main area is titled 'SETTINGS: Choose which part of the graph you want to export. Duplicate rows can optionally be limited to 1 row by checking the "Remove duplicate rows" checkbox (typically where different links have corresponding start and end entities)'. Under 'Export...', the 'Selection only' radio button is selected, marked with a red circle '1'. Below this, the 'Remove duplicate rows' checkbox is unchecked. Under 'Content Format', the 'Grouped by Entity type (human readable)' radio button is selected, marked with a red circle '2'. A 'Preview' table is shown at the bottom, displaying columns A through G with data rows. At the bottom right, the 'Next >' button is highlighted, marked with a red circle '3'.

A	B	C	D	E	F	G
maltego.dark...	Post ID	Domain	Topic Title	Topic ID	Topic Uri	Post Te
EntityID	properties.d...	domain	topic_title	topic_id	topic_uri	text
21cwyjg455...	13087256c2...	dreadditevel...	GOLD PLAT...	13087256c2...	http://dreadd...	http://g...
21cwyjg455...	7173e2c491...	dreadditevel...	Looking for...	7173e2c491...	http://dreadd...	If you h...
21cwyjg455...	99226	darkmarketr...	Sanow novt...	26523	http://darkma...	duoner...
21cwyjg455...	79de1026514...	dreadditevel...	GOLD PLAT...	79de1026514...	http://dreadd...	http://g...
21cwyjg455...	0dc3969c3c...	dreadditevel...	any good pr...	b13770f1b1f...	http://dreadd...	Hi i am...
21cwyjg455...	d9b6b6b9f08...	dreadditevel...	GOLD PLAT...	d9b6b6b9f08...	http://dreadd...	http://g...

File Name & preferred* export format



The screenshot shows the 'Graph Export Wizard' interface at the 'Select File' step. The 'STEPS' sidebar on the left indicates the current step is 'Select File'. The main area is titled 'SELECT FILE: Choose the name, file type and location on your file system to save the table structured file.' Below this, a file explorer window shows the 'Save In' location as 'D:_Webinar\Exports'. The file list contains 'posts 1.csv', 'posts 2.csv', and 'products 1.csv'. At the bottom, the 'File Name' field is set to 'darknet-posts-extract', marked with a red circle '1'. The 'Files of Type' dropdown is set to 'Comma Separated Values (*.csv)', marked with a red circle '2'. At the bottom right, the 'Next >' button is highlighted, marked with a red circle '3'.

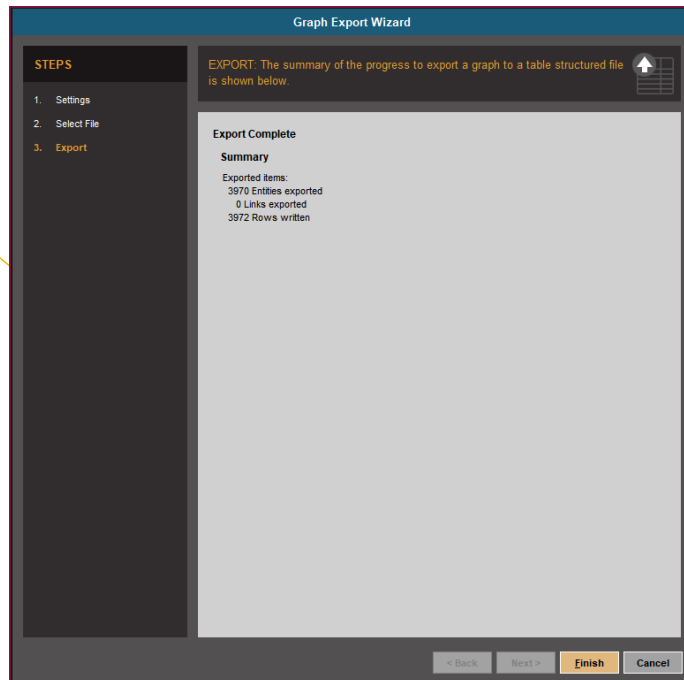
*I prefer „csv“, but feel free to try Excel format. Because...

The following error(s) occurred:
java.lang.IllegalArgumentException: The maximum length of cell contents (text) is 32767 characters

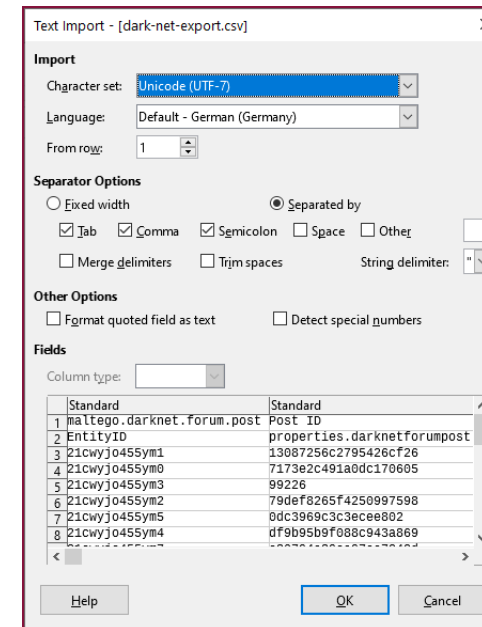
Export Information

Example: Social Links „Dark Net Transforms“

Export as *.csv complete



Import *.csv via Libre Calc*

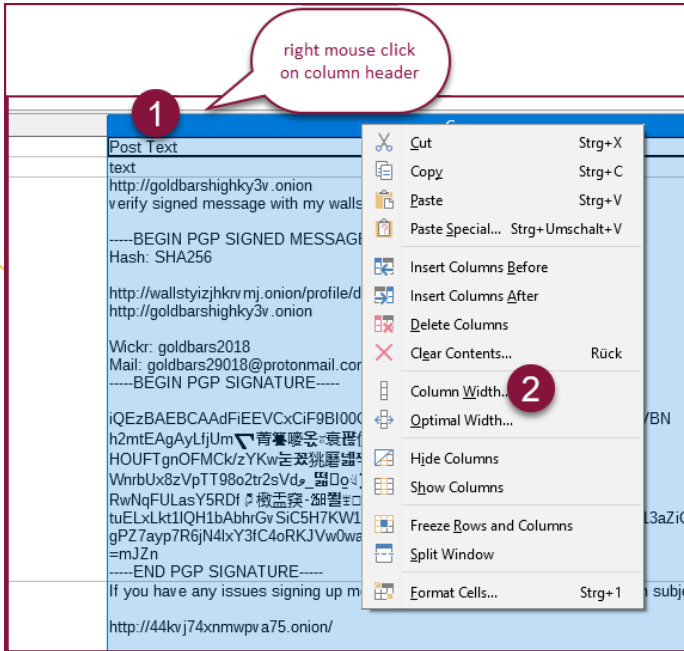


*my preferred way to import csv directly: Libre Office

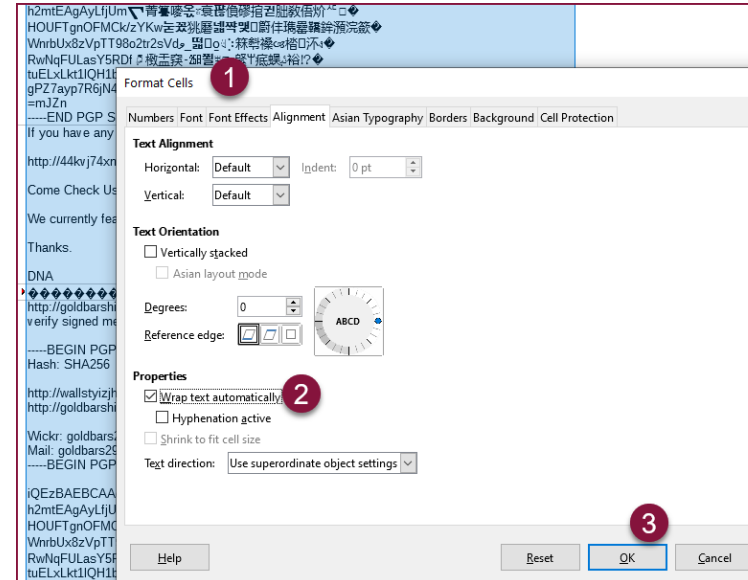
Export Information

Example: Social Links „Dark Net Transforms“

Set Column width for „post text“



Wrap text automatically



Export Information

Example: Social Links „Dark Net Transforms“

Find information

Hey guys we are back and have zepam and Roche available . We are operating	2019-05-23 09:24
Все базы обновлены на 01.06.2019. Напоминаю, что вы можете купить и скачать	2019-06-04 10:57
I am sending out a bunch of 10 pill blisters for free to folks to try and	2018-09-15 10:02
Hello, we are looking for	12 23:07
Hey folks. Just wanted to	24 20:18
We currently have high q	22 15:32
its first time to come here and say Hi to maybe new or old members here . i	2018-03-30 23:44
Lets create a wiki of all the mail services for deepwebbing	either a
Условия: Без посредников. Без предоплаты. 100% конфиденциальность	2017-02-23 20:20

Search Results

Sheet	Cell	Content
dark-net-	\$G\$2885	Maybe open a bank (US) but for UK i dont know if that would wor ^
dark-net-	\$G\$2886	I ordered a paypal account from this guy paypal master on this sit
dark-net-	\$G\$2887	Hi, if i create my own website and put it my own paypal payment I
dark-net-	\$G\$2888	You can get everything on that person, the one on the PayPal acco
dark-net-	\$G\$2889	I will test you with one PayPal account. sand-boxed (browser+ coo
dark-net-	\$G\$2890	Hello, i am also experiencing the same problem, i have tried to lau
dark-net-	\$G\$2891	I do not know, I have never bought a paypal account before, so I a
dark-net-	\$G\$2892	I saw on here a suggestion to use LocalBitcoins, but I ran into a pr
dark-net-	\$G\$2893	In order to add balance throu bank account requires 2 -3 days to r
dark-net-	\$G\$2894	?1 Bitcoin=\$5957 BTCnGame.com 5minutes transfer, 100% trusted /
dark-net-	\$G\$2895	Basically I am looking to buy a paypal account, my aim is to move
dark-net-	\$G\$2896	I'm a beginner in this, for practice I got myself a paypal account w
dark-net-	\$G\$2897	A bitcoin wallet is a device for storing, sending, and receiving bitc
dark-net-	\$G\$2898	where can i get paypal accounts, for free, i know its allot because i

2823 results found (only 1000 are listed)

☒ Show this dialog

Close