

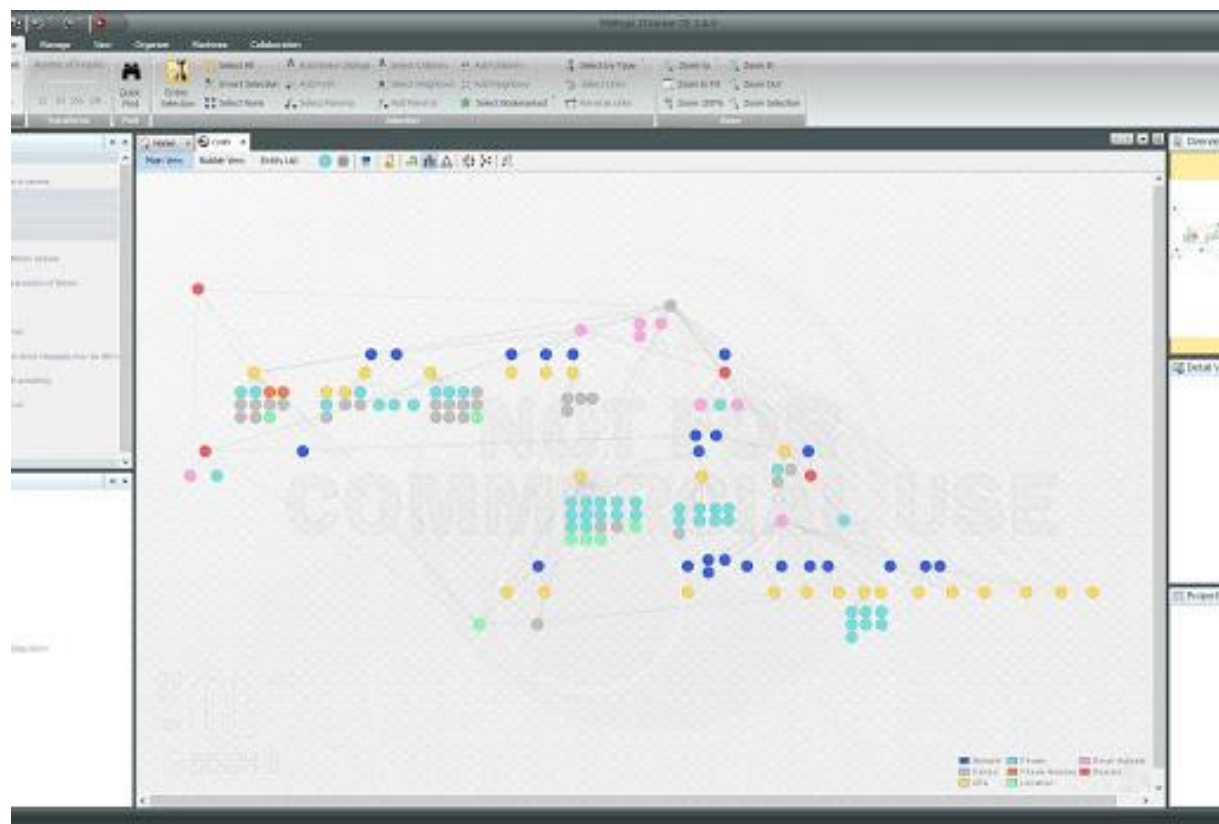
Основные принципы и инструменты OSINT разведки

»SOCIAL MEDIA«

O'SINT



MALTEGO



«Произошла ли утечка персональных данных у кого-нибудь из работников газеты The Guardian?»

- 1) Установить web домены email-адресов работников The Guardian;
- 2) Достать список email-адресов работников The Guardian;
- 3) Сравнить список email-адресов работников The Guardian с данными об утечке и разделить работников на скомпрометированных и не скомпрометированных;
- 4) Составить список работников, чьи данные были найдены в утечке;
- 5) Составить список инцидентов, в которых произошла утечка данных этих работников;
- 6) Составить список типов информации, которая была скомпрометирована.



theguardian

Run Transform(s)

to email

To Email address [From whois info]

To Email addresses [PGP]

To Email addresses

Detail View



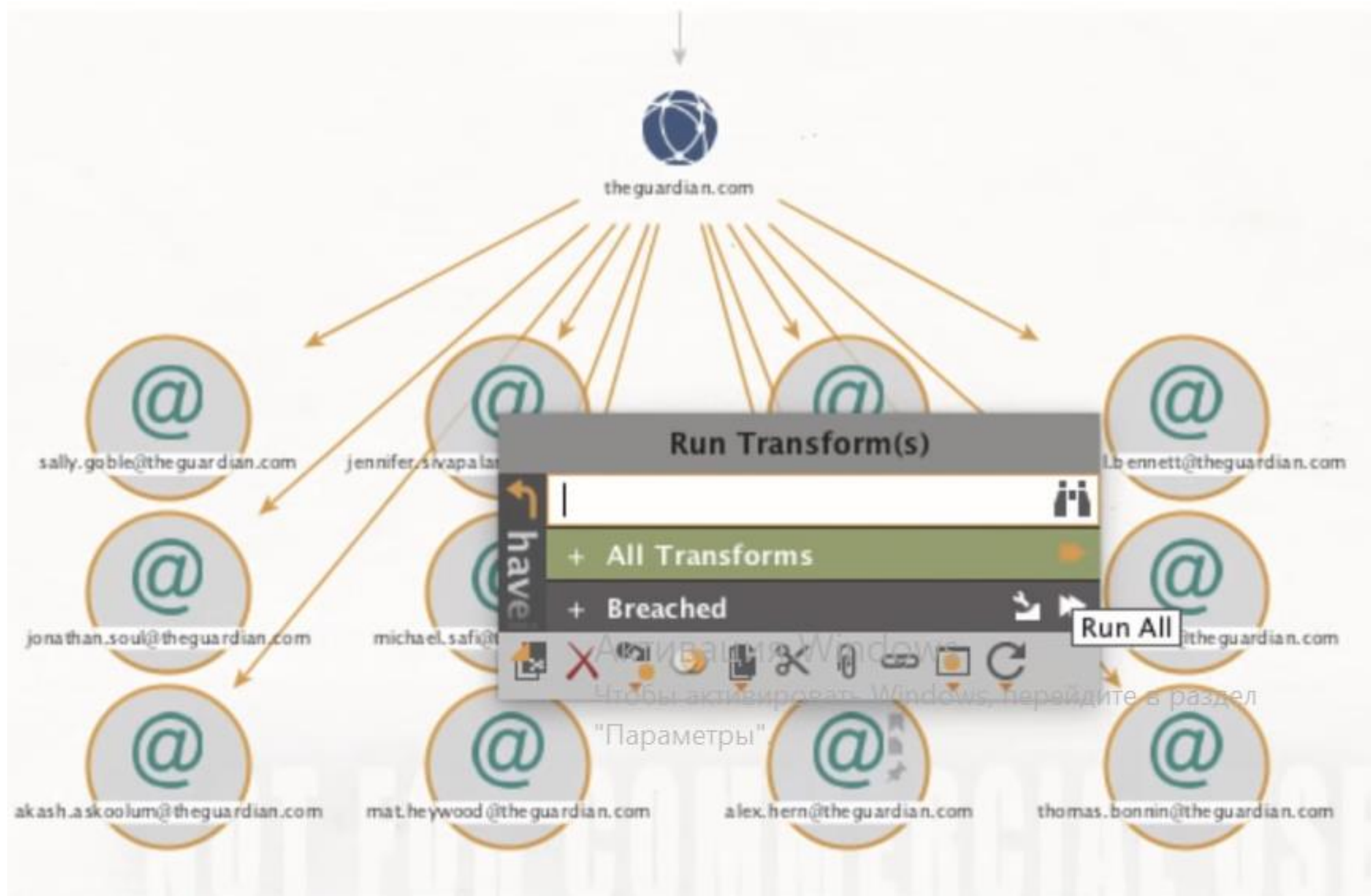
Domain
muhaga.Domain
theguardian.com

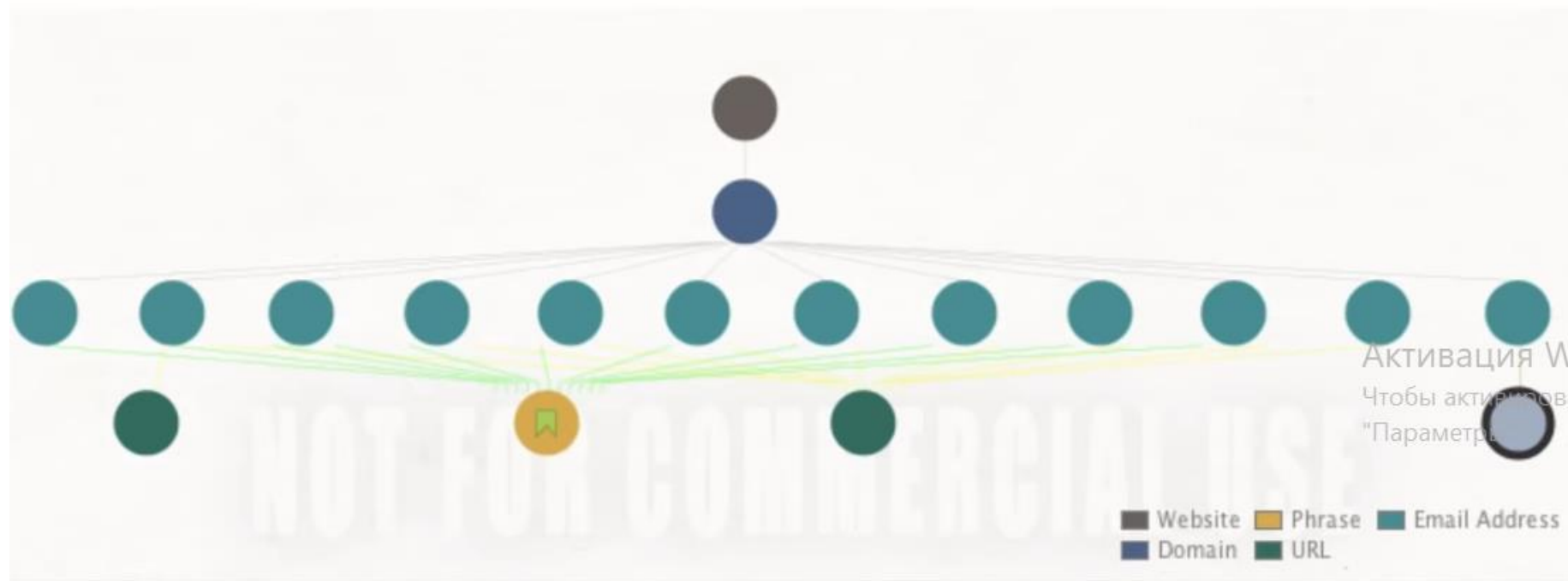
+ Relationships

+ Generator detail

This transform contacts a public PGP keyserver and retrieves email addresses containing the given domain.

Transform





Активация Windows

Чтобы активировать Windows, перейдите в раздел
"Параметры"

+	Entity						
+	@ akash.askoolum@theg				1	1	1...
+	@ alex.hern@theguardian				1	3	1...
+	@ jennifer.sivapalan@the				1	2	1...
+	@ jonathan.soul@thegua				1	2	1...
+	@ justin.pinner@theguar				1	2	1...
+	@ jwhheywood@theguar				1	2	1...
+	@ michael.safir@theguard				1	2	1...
+	@ nathaniel.bennett@the				1	2	1...
+	@ sally.goble@theguardi				1	2	1...

9 of 27 entities



t@theguardian.com



akash.askoolum@theguardian.com



regis.kuckaertz@theguardian.com

15 December 2016 - PayAsUGym

In December 2016, an attacker breached PayAsUGym's website exposing over 400k customers' personal data. The data was consequently leaked publicly and broadly distributed via Twitter. The leaked data contained personal information including email addresses and passwords hashed using MD5 without a salt.



IP addresses



Names



Browser user agent details



Email addresses



Phone numbers



Website activity



Partial credit card data



Passwords

Активация Windows

Чтобы активировать Windows, перейдите в раздел "Параметры".



Основные принципы OSINT разведки

- Вопрос поставлен корректно, на него можно дать конкретный ответ
- Все действия логичны и последовательно идут друг за другом
- Собранные данные обработаны, пропущены через контекст
- На выходе был получен ответ а также определена дальнейшая схема действий

OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND
ANALYZING ONLINE INFORMATION

EIGHTH EDITION

Michael Bazzell

