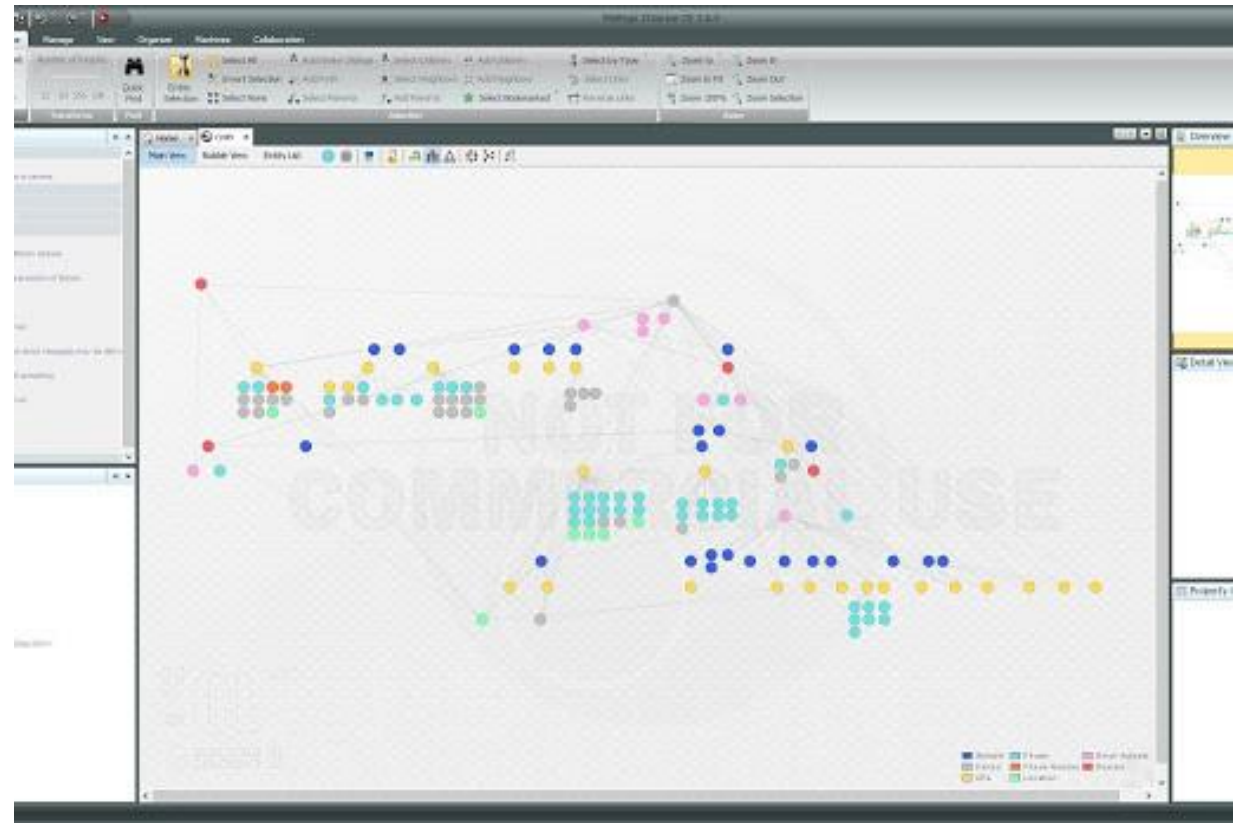
Основные принципы и инструменты OSINT разведки


»SOCIAL MEDIA«
O·SINT

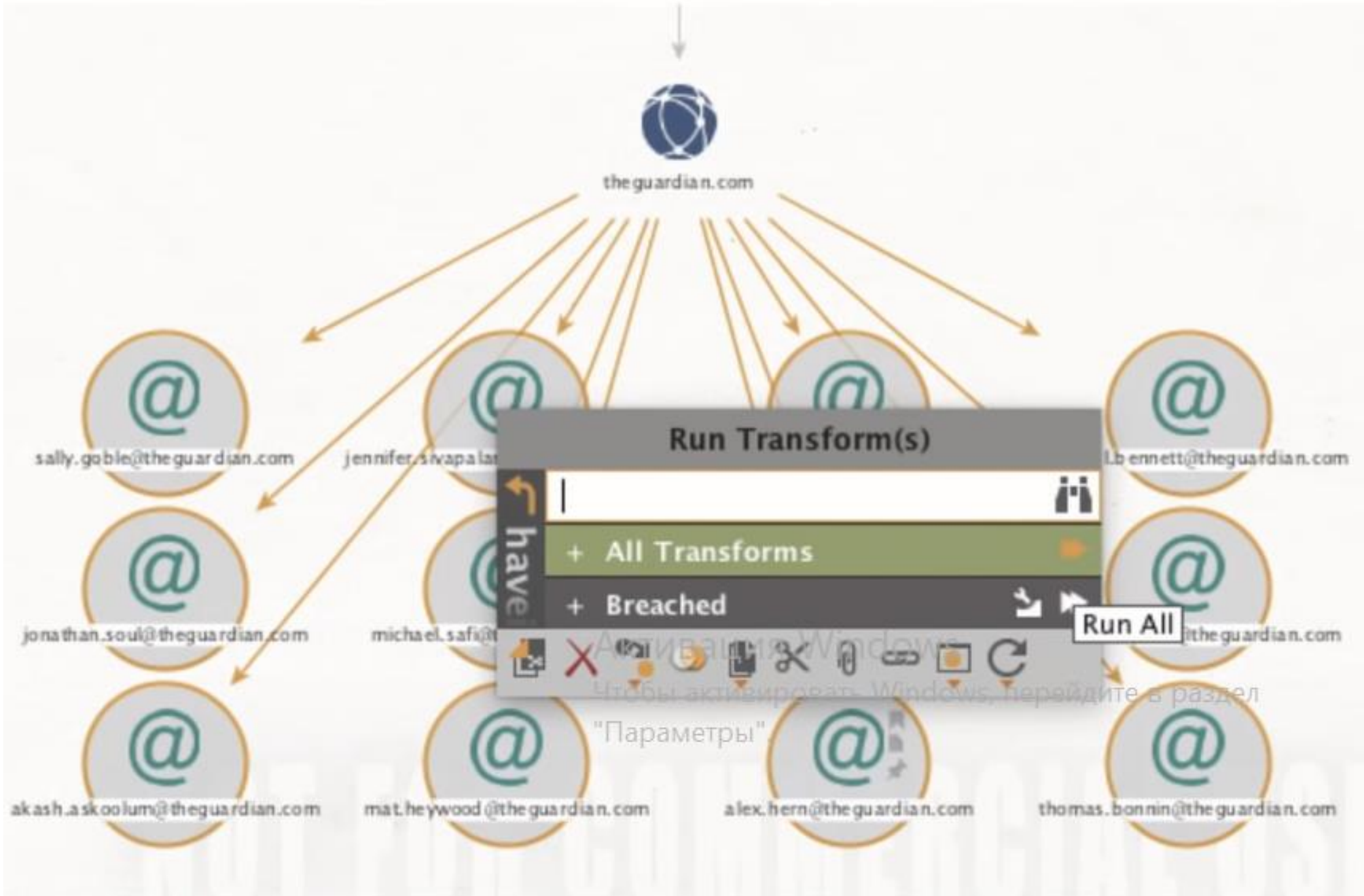
MALTEGO

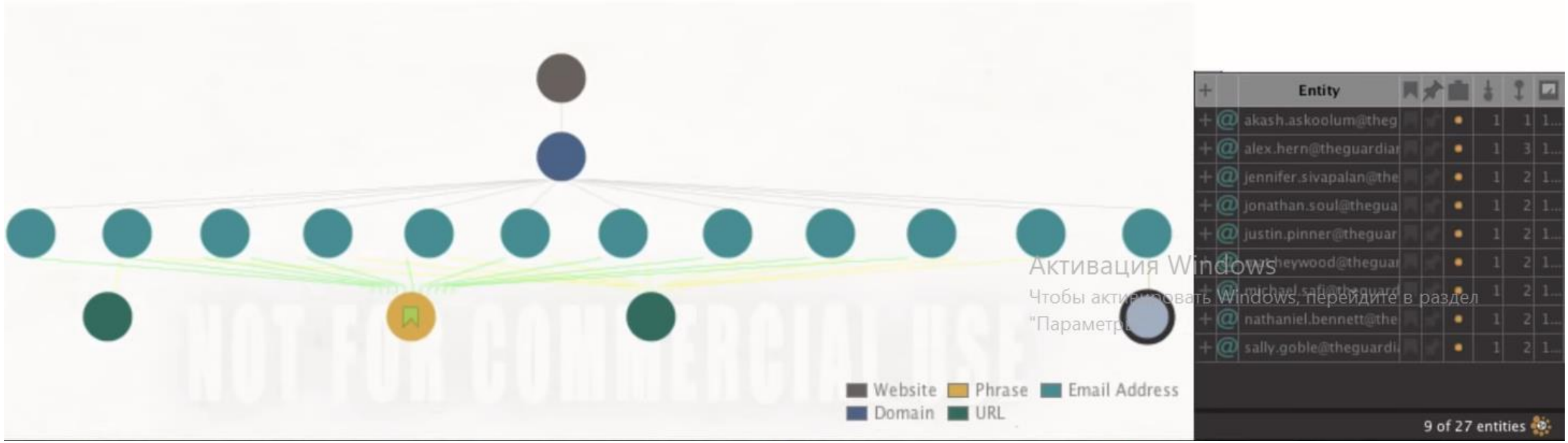


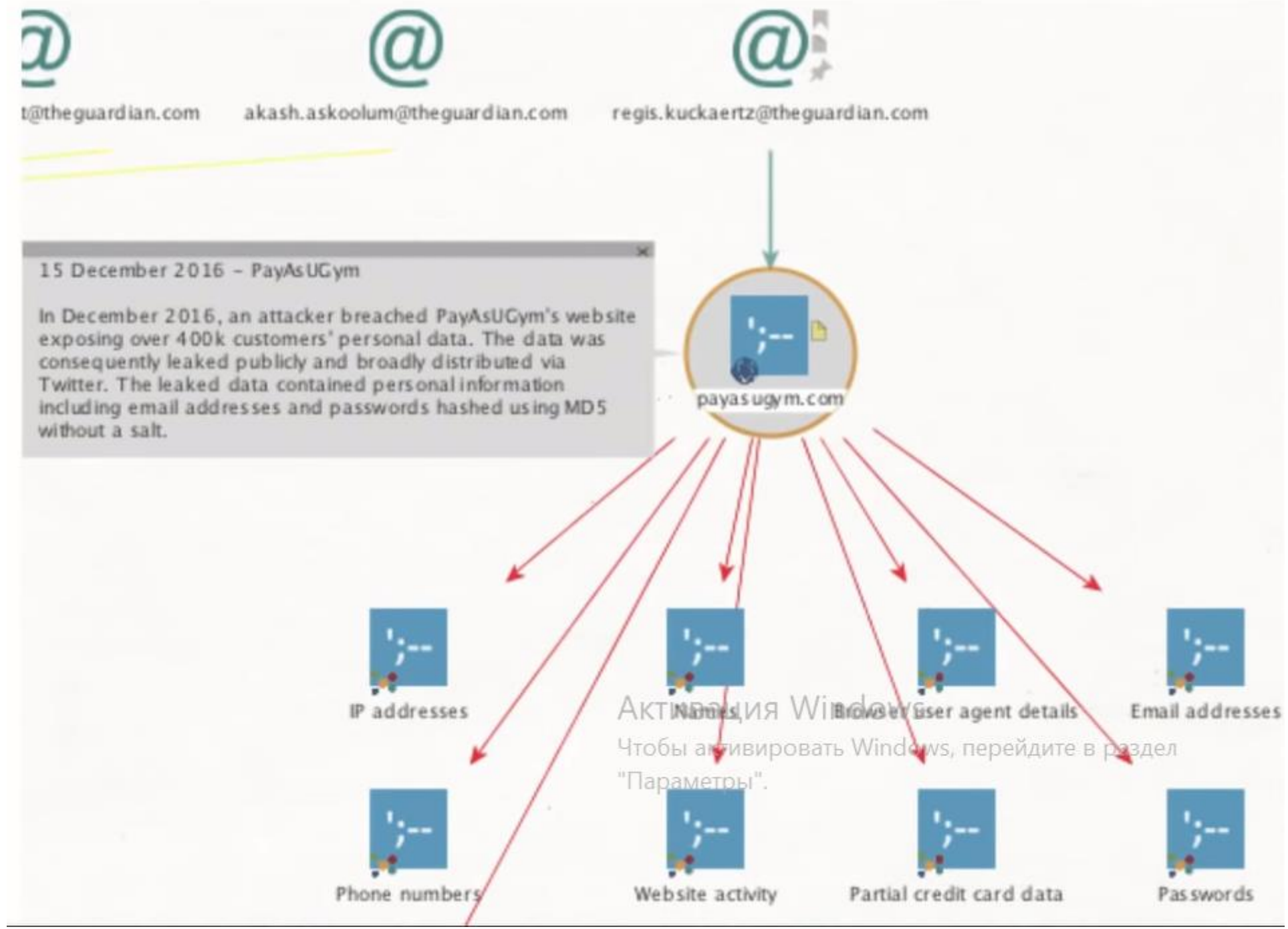
«Произошла ли утечка персональных данных у кого-нибудь из работников газеты The Guardian?»

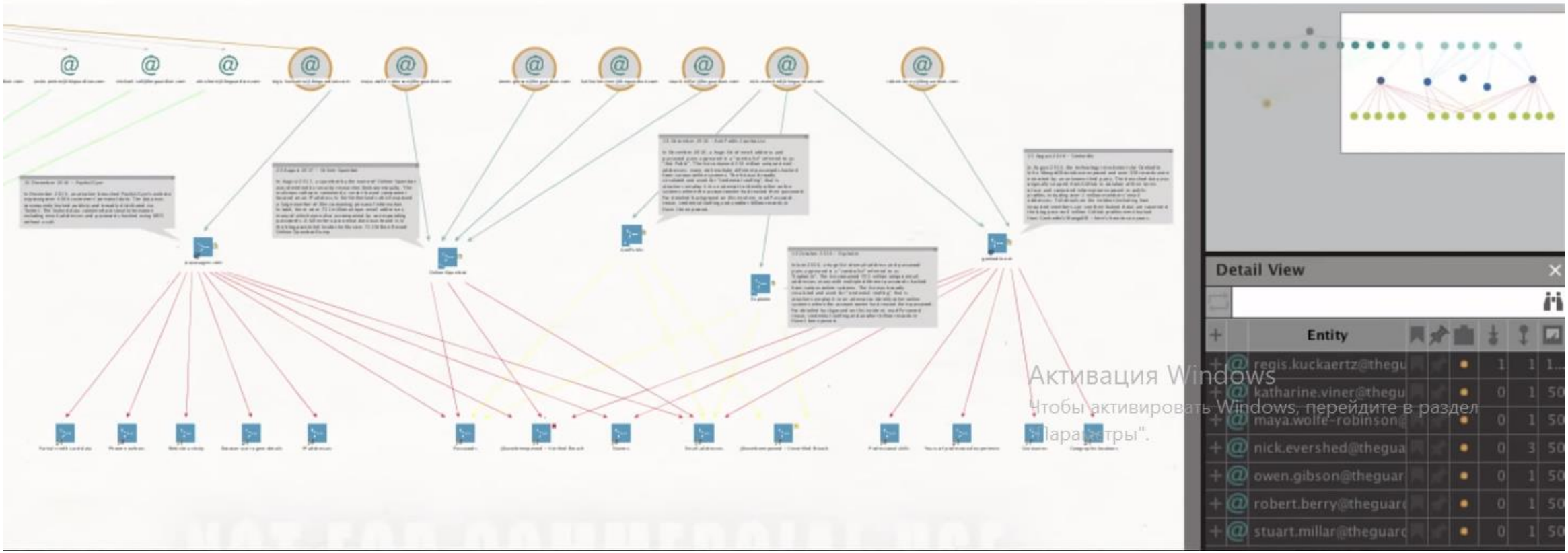
- 1) Установить web домены email-адресов работников The Guardian;
- 2) Достать список email-адресов работников The Guardian;
- 3) Сравнить список email-адресов работников The Guardian с данными об утечке и разделить работников на скомпрометированных и не скомпрометированных;
- 4) Составить список работников, 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.


Run Transform(s)
to email
To Email address [From whois info]
To Email addresses [PGP]
This transform contacts a public PGP keyserver and retrieves email addresses containing the given domain.
Detail View
Domain
theguardian.com
+ Relationships
+ Generator detail


theguardian.com
sally.goble@theguardian.com
jonathan.soul@theguardian.com
akash.askoolum@theguardian.com
mat.heywood@theguardian.com
alex.hern@theguardian.com
thomas.bonnin@theguardian.com
Run Transform(s)
+ All Transforms
+ Breached
Run All







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