CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Alexandre Ribeiro
Analista de Incidentes

4º Fórum Brasileiro de CSIRTs

17 de setembro de 2015

Objetivos

- Apresentar os aspectos iniciais do trabalho de pesquisa sobre a possível aplicação da análise de redes sociais;
- Trocar experiências com outros times.

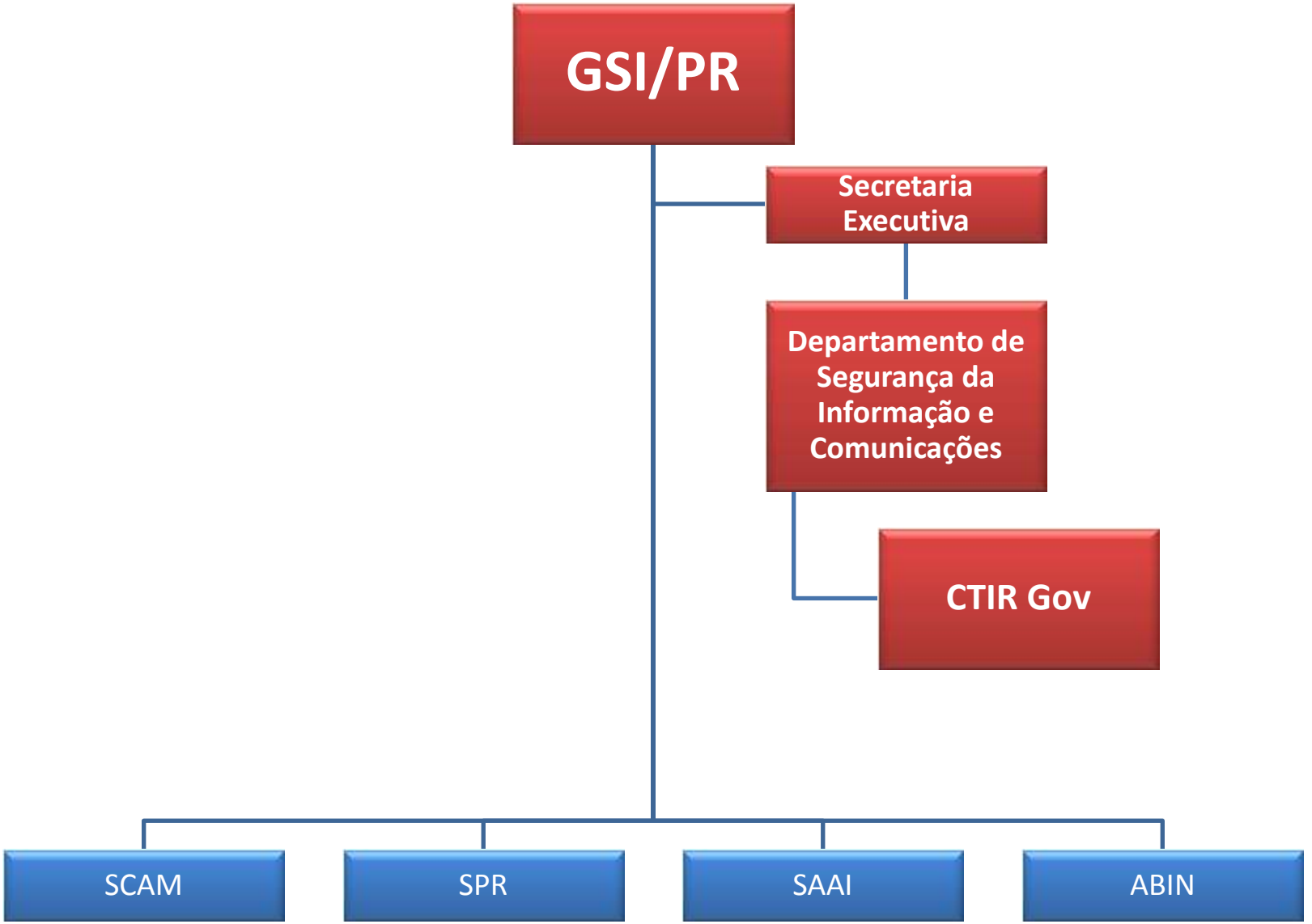
Sumário

Agenda

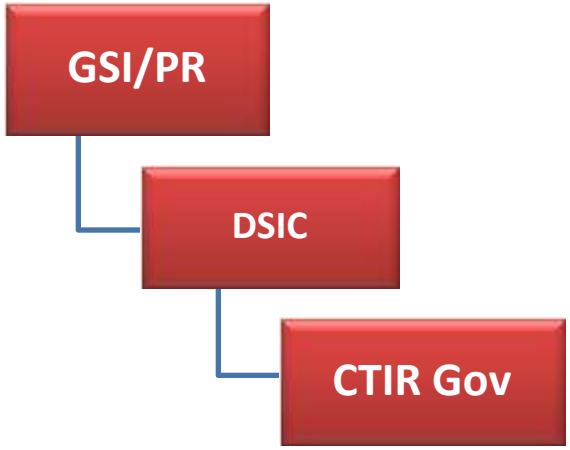
- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

CTIRGov

Ambientação



Ambientação



LEI Nº 10.683, DE 28 DE MAIO DE 2003.

CAPÍTULO I
DA PRESIDÊNCIA DA REPÚBLICA
Seção I
Da Estrutura

Art. 1º A Presidência da República é constituída, essencialmente:

VI - pelo Gabinete de Segurança Institucional;

Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete:

IV - coordenar as atividades de inteligência federal e de segurança da informação;

DECRETO Nº 5.772, DE 8 DE MAIO DE 2006. (revogado)
DECRETO Nº 6.931, DE 11 DE AGOSTO DE 2009. (revogado)
DECRETO Nº 7.411, DE 29 DE DEZEMBRO DE 2010. (revogado)

DECRETO Nº 8.100, DE 4 DE SETEMBRO DE 2013

Aprova a Estrutura Regimental Cargos e Funções

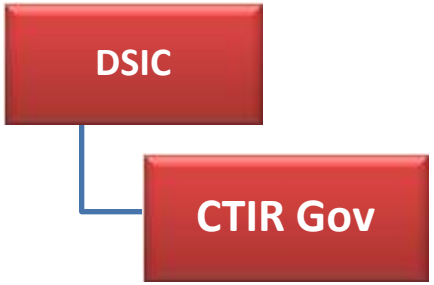
CAPÍTULO III
DAS COMPETÊNCIAS DOS ÓRGÃOS
Seção I

Art. 6º Ao Departamento de Segurança da Informação e Comunicações compete:

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

CTIRGov

Ambientação



GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 56, DE 5 DE NOVEMBRO DE 2009

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art. 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov);

II - promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores junto a outros centros;

III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

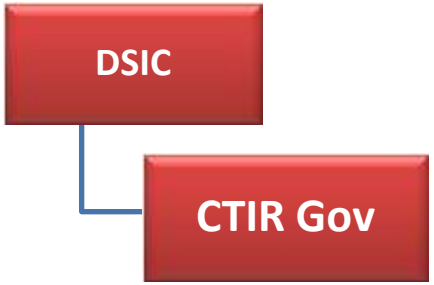
IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

CTIRGov

Ambientação



- ✓ **Centro de Coordenação Nacional**
- ✓ **Comunidade de Tratamento de Incidentes do CTIR Gov**
  - APF direta e indireta
  - excepcionalmente, Estados e Municípios
  - “gov.br”, “jus.br”, “leg.br”, “mil.br”, “mp.br” e outros (ex: algumas empresas “.com.br”).

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 56, DE 5 DE NOVEMBRO DE 2009

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art. 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov);

II - promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores junto a outros centros;

III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

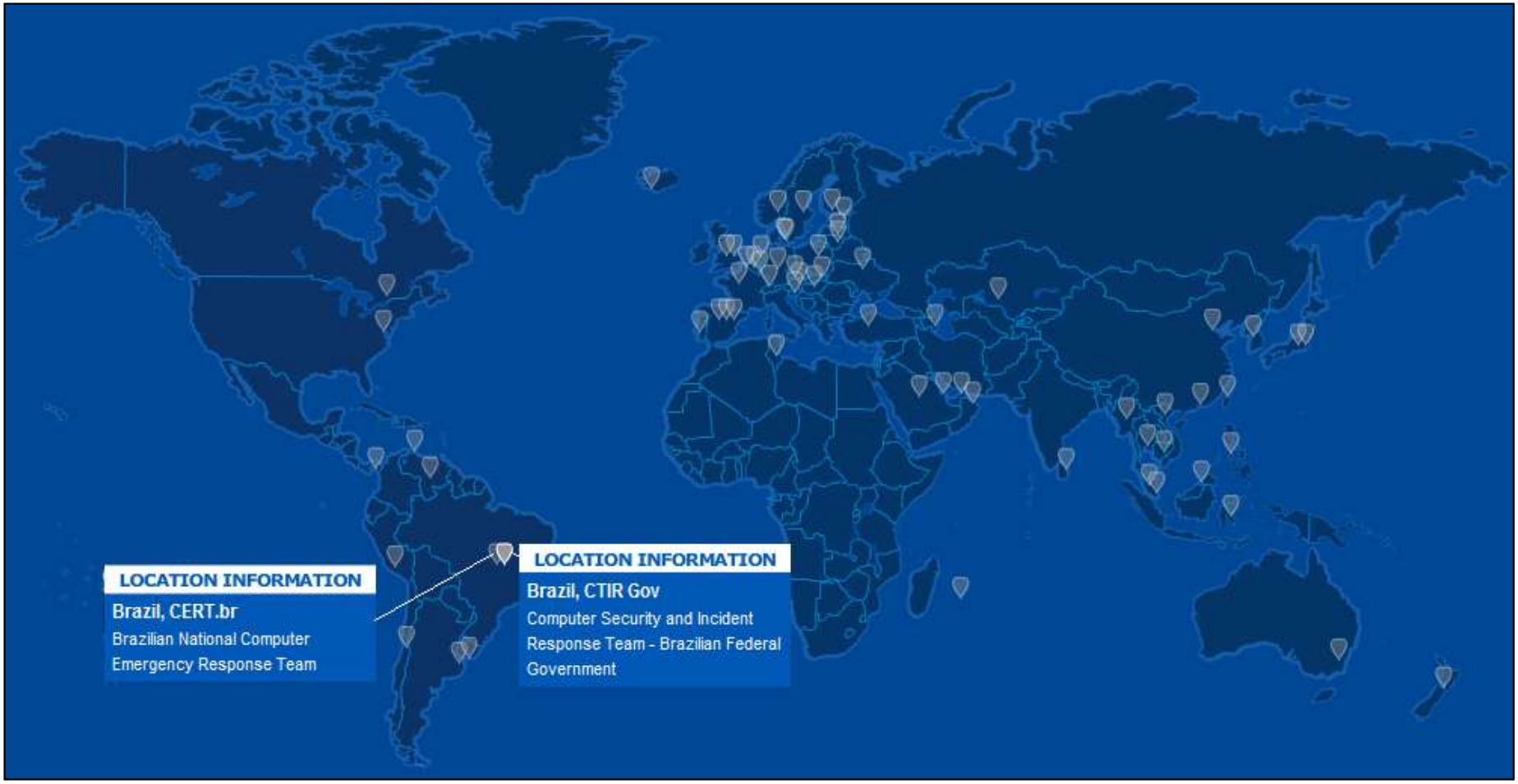
IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

Ambientação

Centros de tratamento com responsabilidade nacional



Fonte: http://www.cert.org/csirts/national/

CTIR Gov

Sumário

Agenda

- ✓ Ambientação
- ✓ **Definição do tema**
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

CTIR Gov

O tema de pesquisa

Tópicos Especiais em Comunicação e Mediação da Informação, Fundamentos da Ciência de Redes e Análise de Dados em Redes Complexas

Identificação de Ameaças ao Estado Brasileiro a partir da Análise de Redes Sociais

Grupo de Trabalho:

Alexandre J. Ribeiro, Adão dos Santos, Claudio G. Bernardo, Marcelo A. B. Oliveira

Prof. Dr. **Ricardo Sampaio**

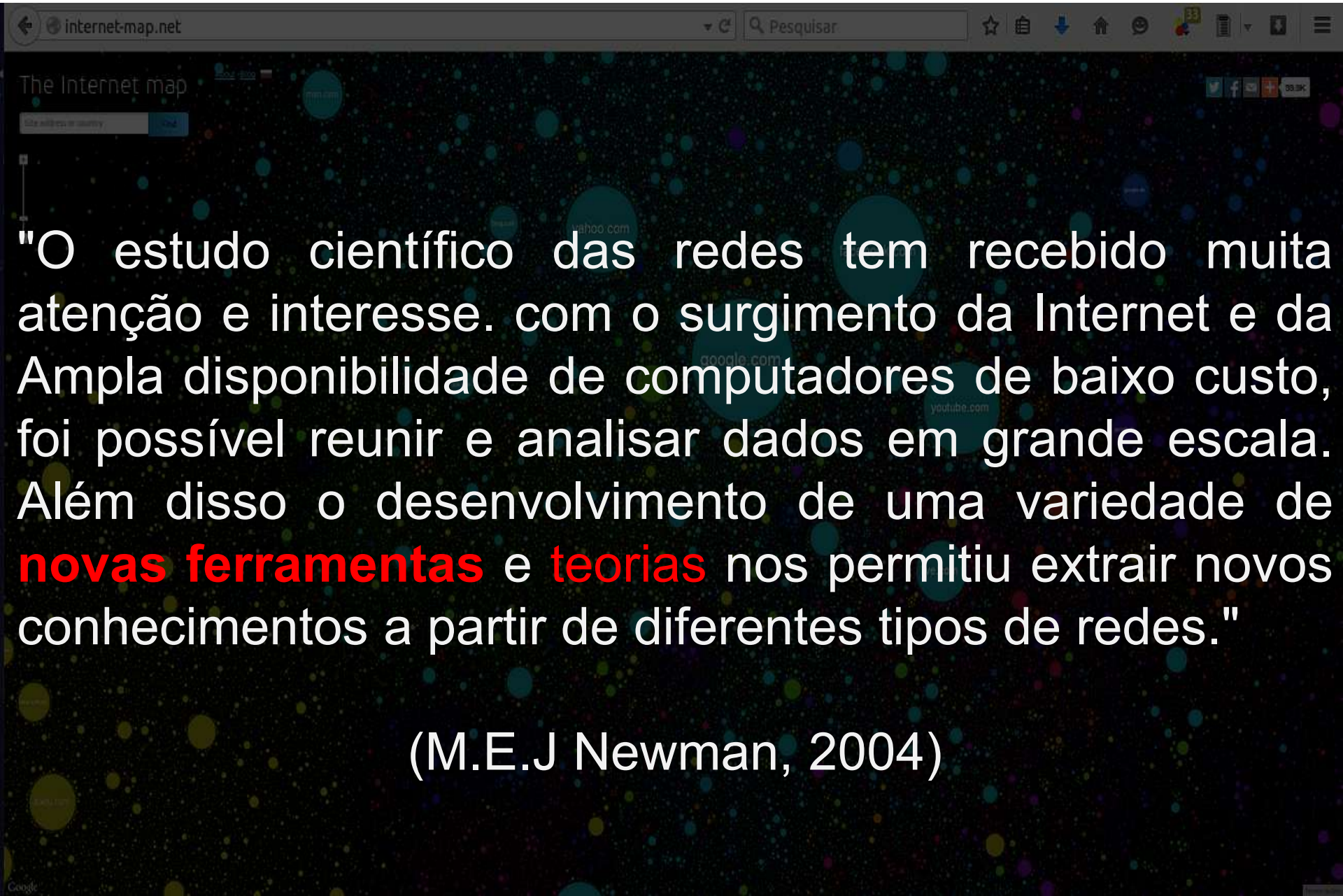
Julho de 2015

CTIRGov

Justificativa

Possibilidade de aplicação da Análise de Redes Sociais (ARS) como ferramenta de inteligência na prevenção de ataques a sítios e/ou a infraestruturas críticas do Estado Brasileiro.

O estudo da redes



"O estudo científico das redes tem recebido muita atenção e interesse. com o surgimento da Internet e da Ampla disponibilidade de computadores de baixo custo, foi possível reunir e analisar dados em grande escala. Além disso o desenvolvimento de uma variedade de **novas ferramentas** e teorias nos permitiu extrair novos conhecimentos a partir de diferentes tipos de redes."

(M.E.J Newman, 2004)

Sumário

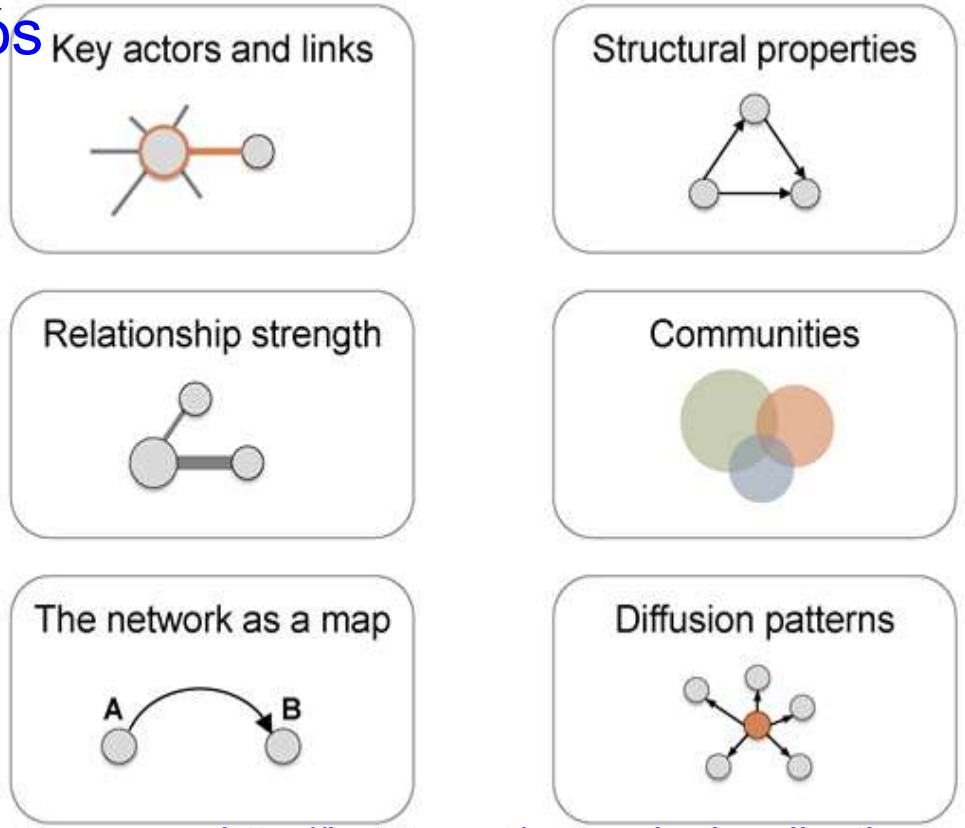
Agenc

- ✓ Ambientação
- ✓ Definição do tema
- ✓ **A ciência de redes**
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

Ciência de Redes

De forma simplificada, uma rede pode ser definida como: "**Um conjunto de pontos interligados**"

- Um conjunto de vértices ou nós com conexões entre eles, denominadas de arestas (Newman, 2003).
- Os nós podem ser pessoas, organizações, equipamentos, locais, etc.
- As linhas ou arestas formam os relacionamentos



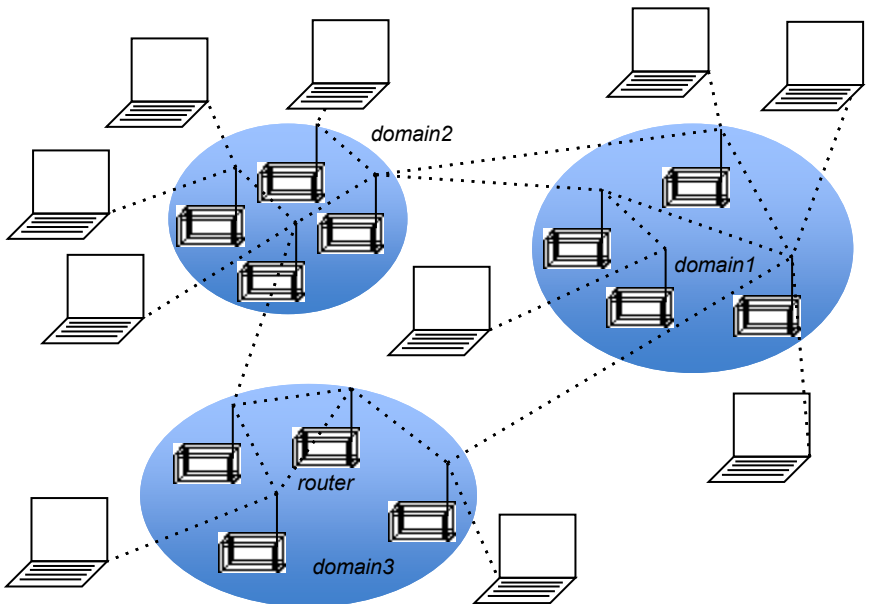
http://kateto.net/network-visualization

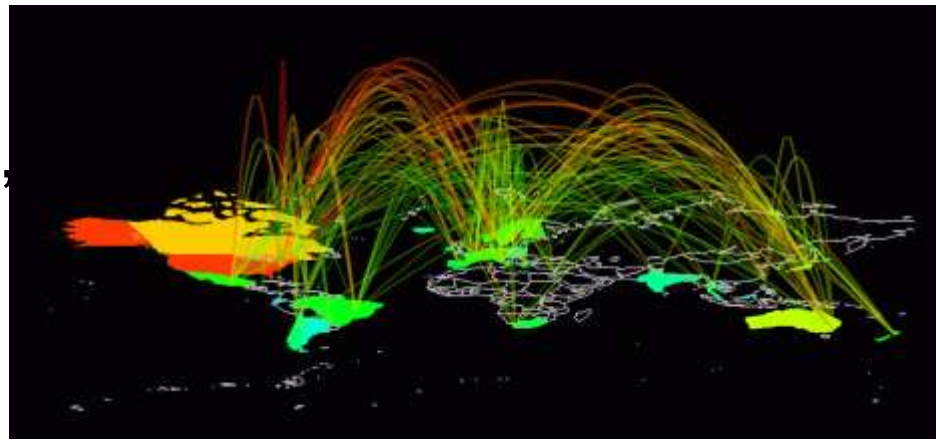
CTIRGov

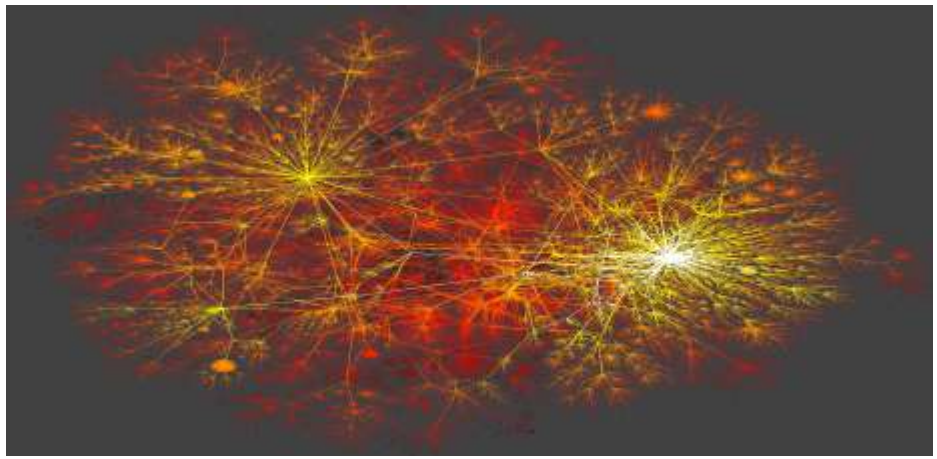
Ciência de Redes

- As redes são fundamentadas:
  - construção teórica da Sociologia, com fundamentação matemática da teoria do grafos.

- Podem ser: tecnológicas, de informação, biológicas, sociais, etc.



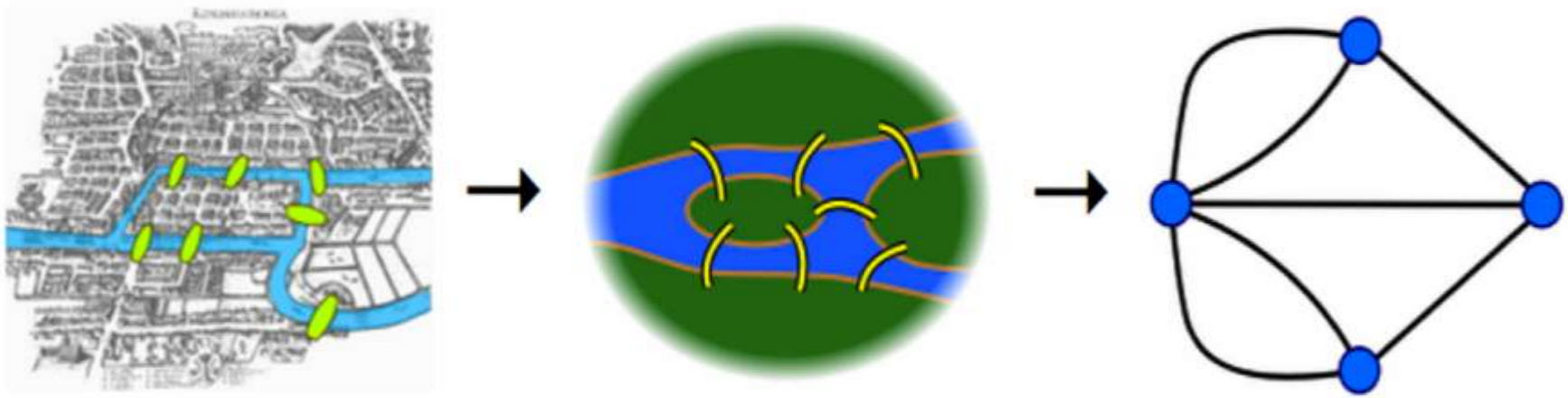




Referências históricas

Leonhard Euler's Theory (1735)

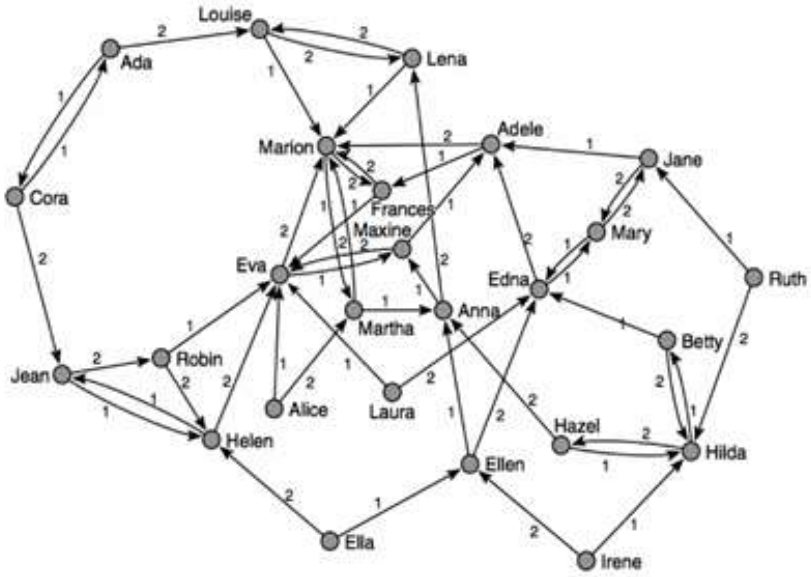
7 pontes de Königsberg

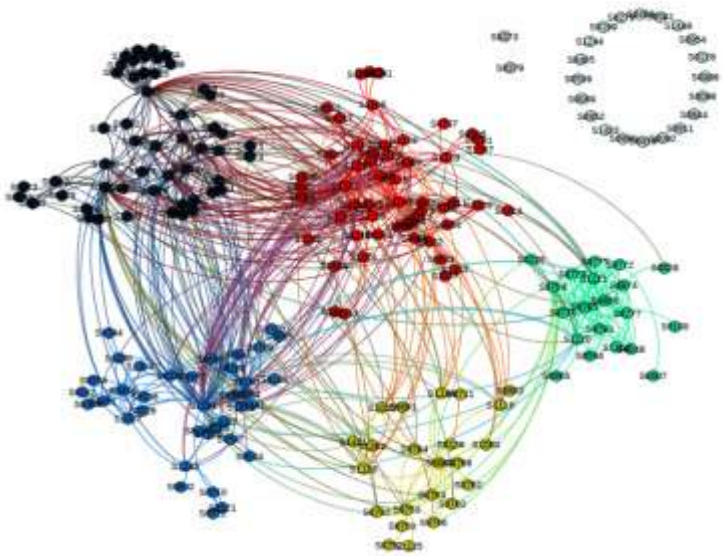


Referências históricas

Estudo Empírico das Redes

Jacob, Moreno, 1930 - Sociogramas:
"A simples visualização de uma rede pode trazer muitas informações."





CTIRGov

Referências históricas

Stanley Milgram - Experimento - 1969

Stanley Milgram - Pesquisa sobre a distância média entre as pessoas também conhecido como "Seis Graus de Separação"

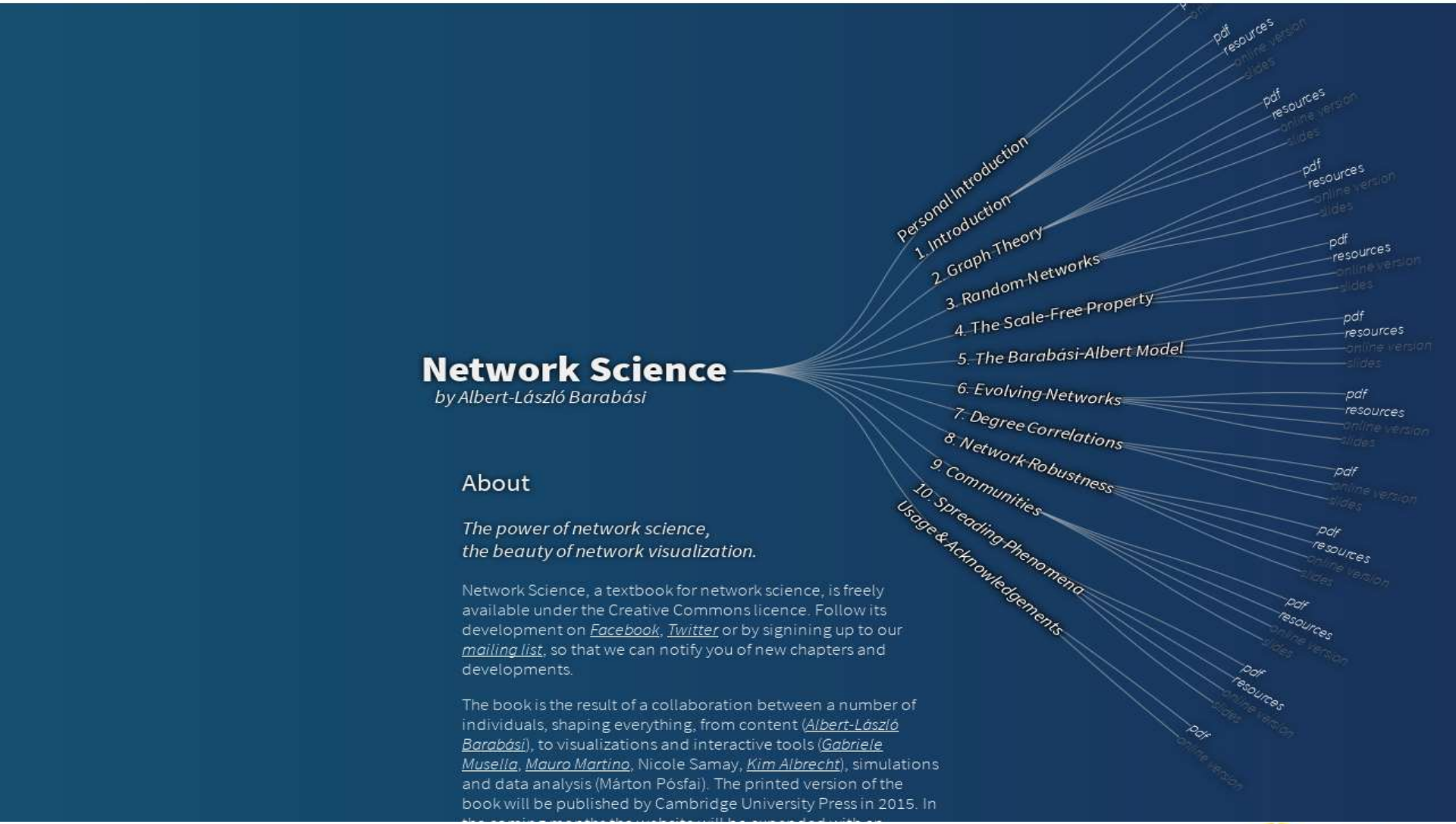
Marcos principais

Linha do Tempo

1735	1930	1950	1954	1967	1988
Teoria do grafos teve início quando Leonhard Euler propôs uma solução para o problema das pontes de Königsberg,	Jacob Moreno desenvolve a Sociometria , segundo a qual, o núcleo social é na verdade o indivíduo e seus relacionamentos, sociais, econômicos e culturais.	•Manfred Kochen - Manuscrito sobre •Teoria da Redes Sociais e experimento e "redes Small-word" publicado em 1978.	• Prof. J A. Barnes Adota o termo "Redes Sociais" para definir os laços sociais (relacionamentos) objetos de sua pesquisa.	•Stanley Milgran e o experimento "Small-word"- que demonstou que qualquer pessoa poderia ser alcançada em seis passos (six-degrees of separation).	• Surge a "Al Qaeda" 

1994	1998	1998	2001	2003	2006
• Quatro estudantes desenvolvem o Game "Six Degree of Kevin Bacon"	• Watt e Strogatz Revivem o experimento de Milgran no artigo "Colletictive Dynamics of small-world networks.	Google Novo buscador "New Search engine that's ranks pages according to their relationship with anothers"	• Lançamento da Wikipedia Al Qaeda lança os ataques de 11 Set.	• Captura de Saddan Hussein **2004** facebook **2005** YouTube	twitter **2010** Primavera Árabe 

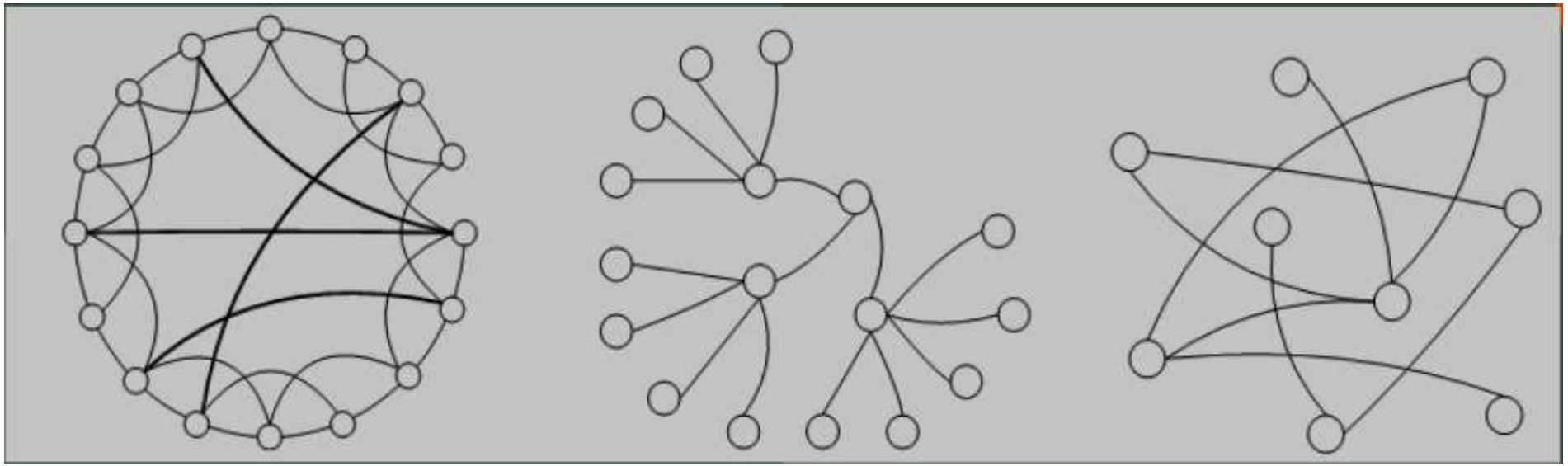
Ciência de Redes - A. Barabási



http://barabasi.com/networksciencebook/

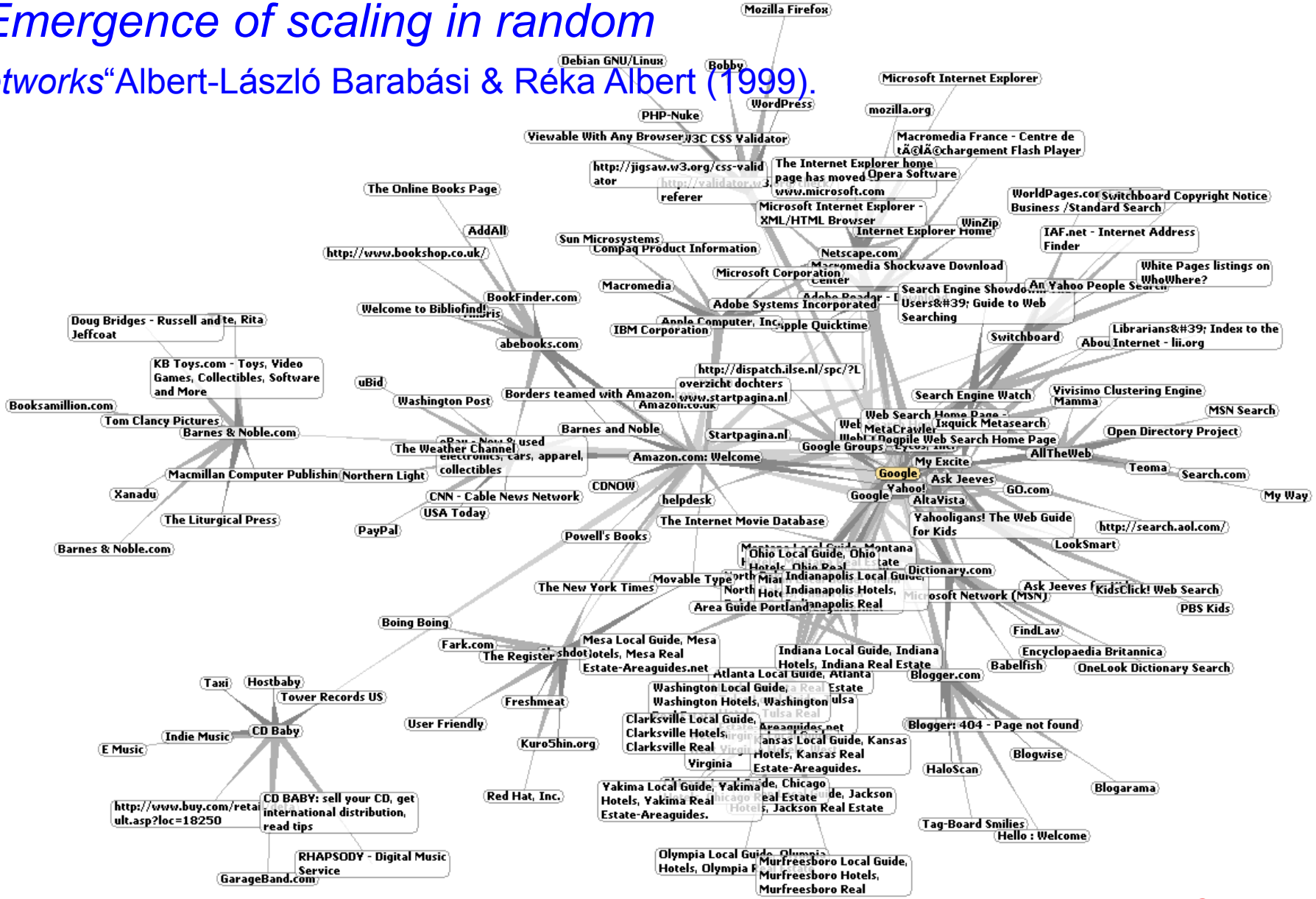
Estrutura das redes

- As redes complexas podem ser:
  - Redes Randômicas - Erdos Y Reny (1959)
  - Redes Mundo-pequeno (Small-Word) - Watts and Strogatz (1998);
  - Redes Livres de Escala - possui como uma das principais características, conexão preferencial. – Barabasi (2001).



Redes Livres de Escala

"*Emergence of scaling in random networks*"Albert-László Barabási & Réka Albert (1999).



https://upload.wikimedia.org/wikipedia/commons/c/ce/WorldWideWebAroundGoogle.png

Sumário

Agenda

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ **Análise de Redes Sociais - ARS**
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

CTIR Gov

Macro processos da análise de rede

- Definição da rede;
- Manipulação da rede;
- Determinação das características estruturais;
- Inspeção visual.

Propriedades de análise de redes

Centralidade:

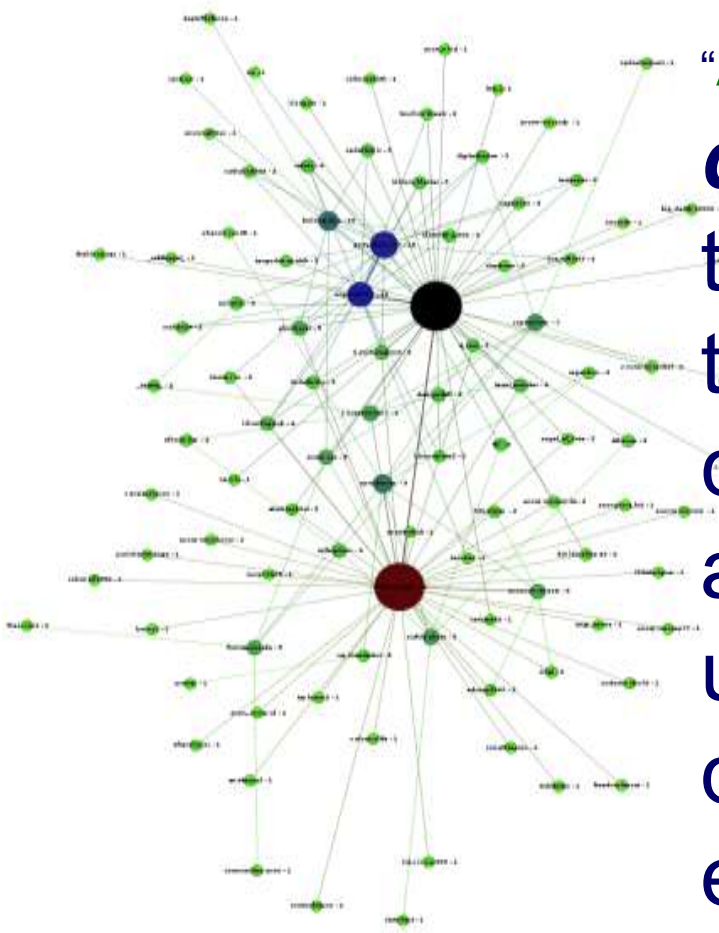
- Grau, Proximidade, Intermediação e Autovetor.

PageRank:

- Algumas medidas foram criadas com foco nas páginas WEB.
- Criada pelos fundadores do Google: Laurence Page e Sergey Brin.
- Uma página se torna “central” quando outras páginas importantes mencionam ou fazem links para esta página.

Modularidade: Grau de agrupamento dos nós.

Centralidade de Grau

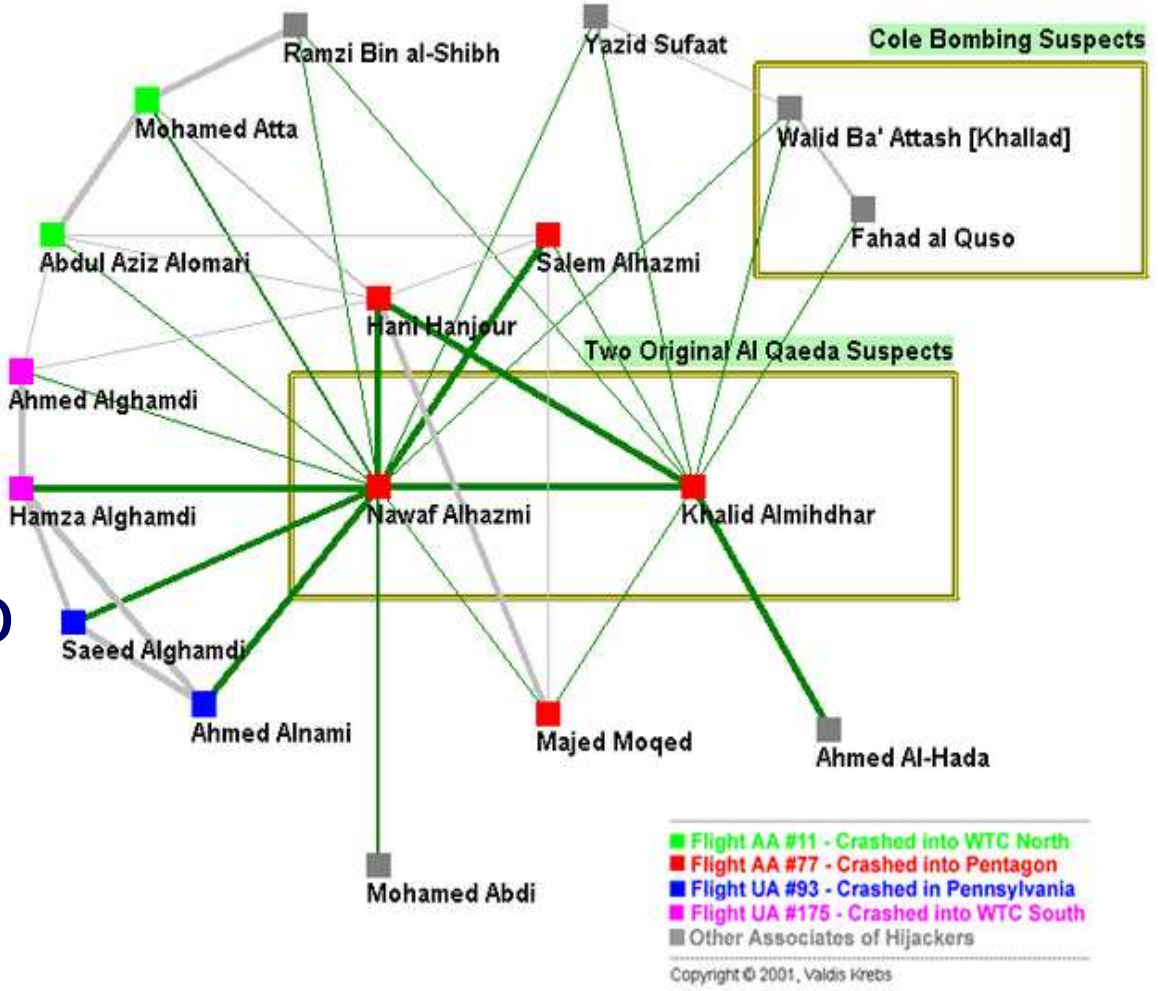


"A centralidade de grau ou ***degree centrality*** é talvez a mais simples de todas as medidas de centralidade, esta métrica avalia a importância de um nó analisando a quantidade de nós a que ele é ligado".
(RONQUI, 2014)

Centralidade de Intermediação

Betweenness

Apresenta os elementos que estão em posição de interligação na rede, na medida em que eles estão no menor caminho entre diferentes *clusters*.

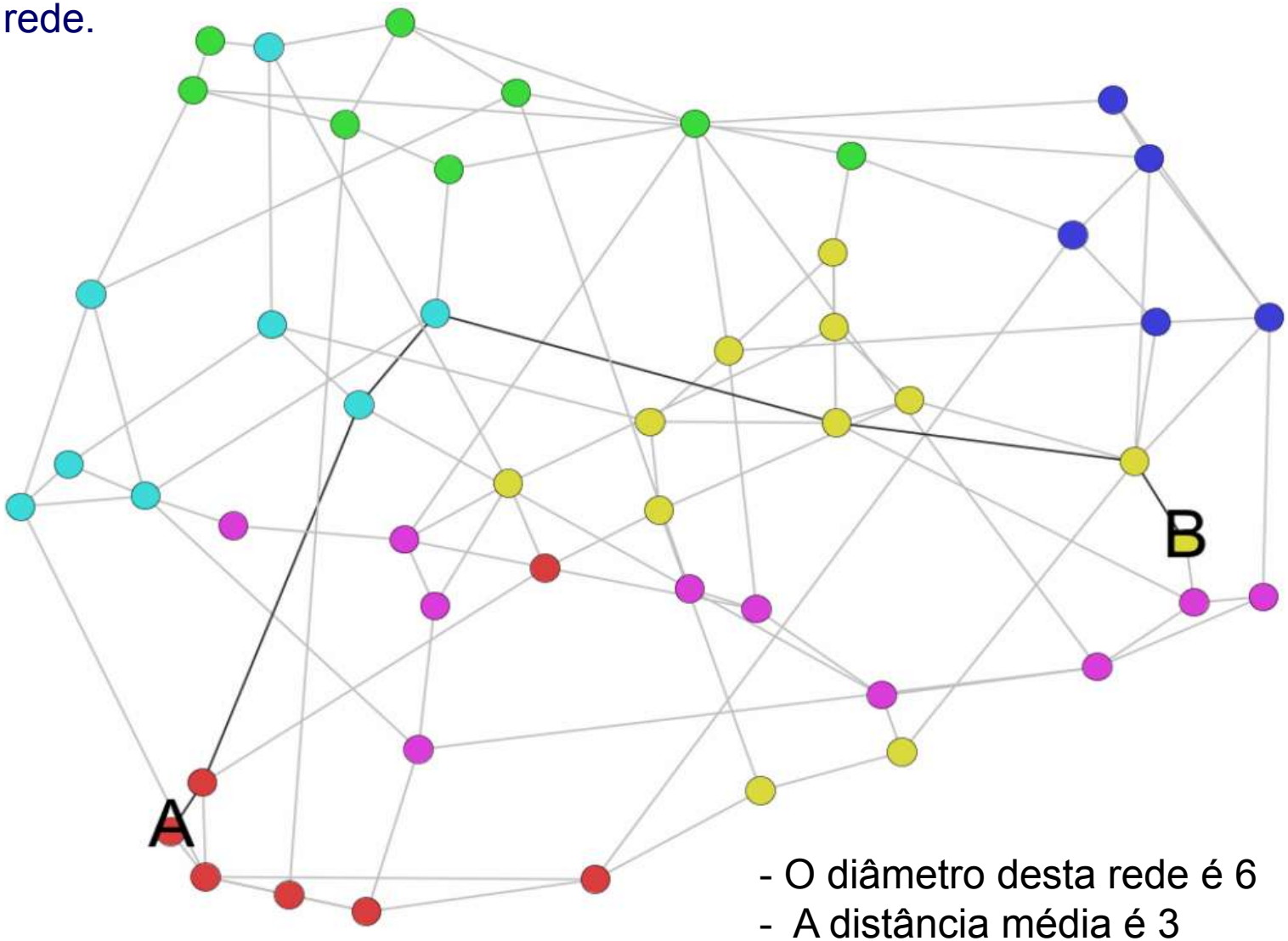


http://nationalsecurityzone.org/war2-0/case-studies/september-11-hijackers/

Figure 2 - All nodes within 1 step [direct link] of original suspects

Diâmetro da rede

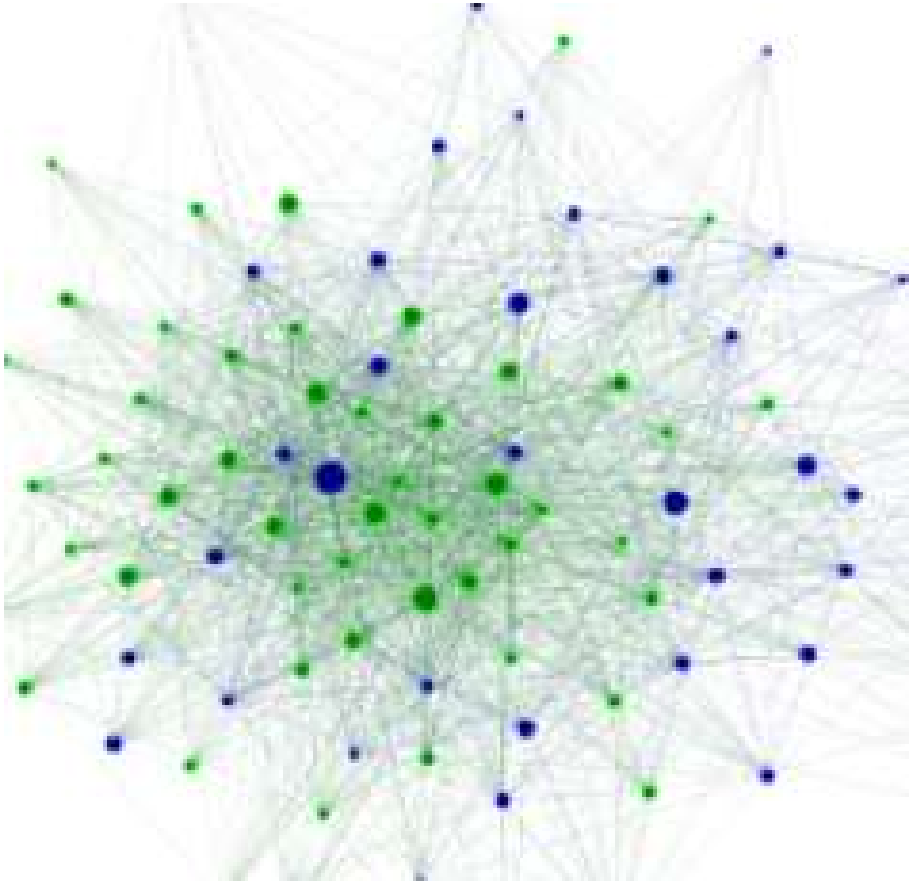
Distância máxima entre dois vértices, sendo o maior caminho mínimo (geodésico) entre dois vértices da rede, simbolizando o nível de ligação entre os vértices da rede.



- O diâmetro desta rede é 6
- A distância média é 3

Densidade da rede

A densidade de uma rede é calculada com base no número de linhas que esta possui dividido pelo número máximo possível de linhas para esta rede

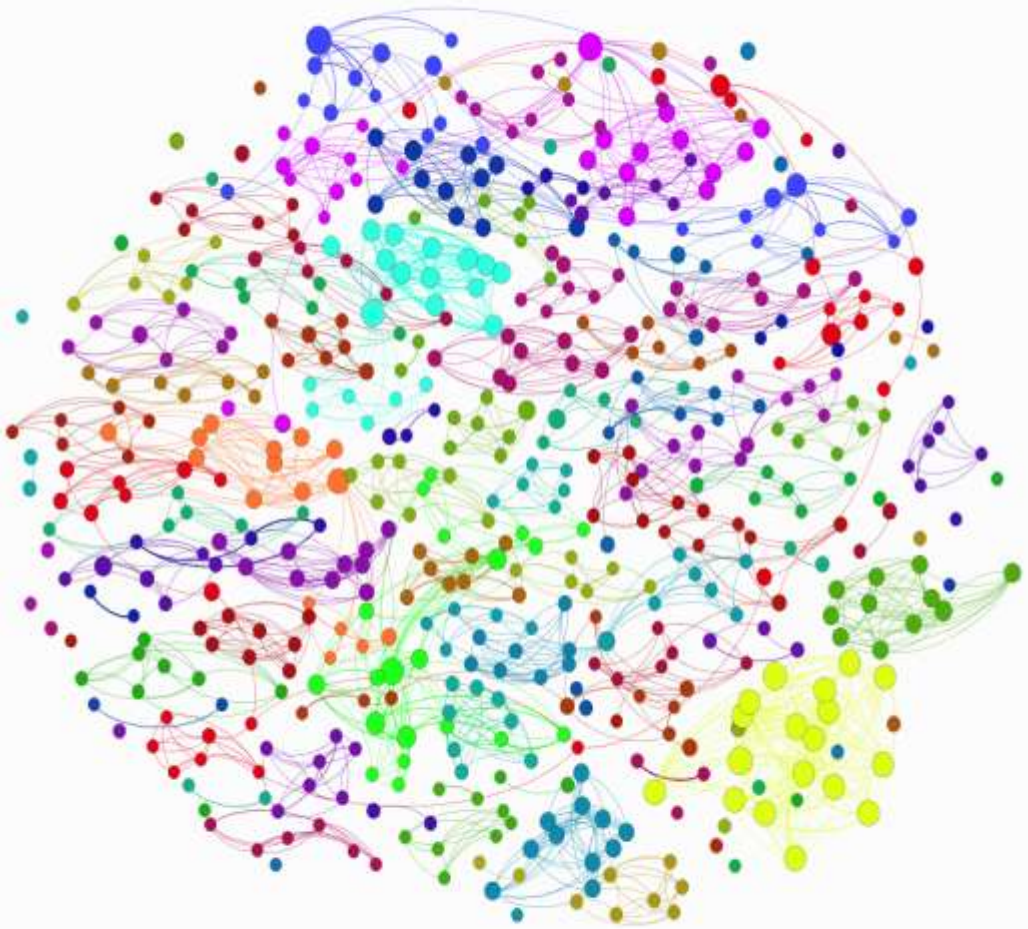


CTIRGov

Coeficiente de clusterização

- É uma medida do grau em que os nós em um grafo tendem a se agrupar.

- Os nós tendem a criar grupos coesos caracterizados por uma densidade relativamente alta, (Holland e Leinhardt, 1971; Watts e Strogatz, 1998)

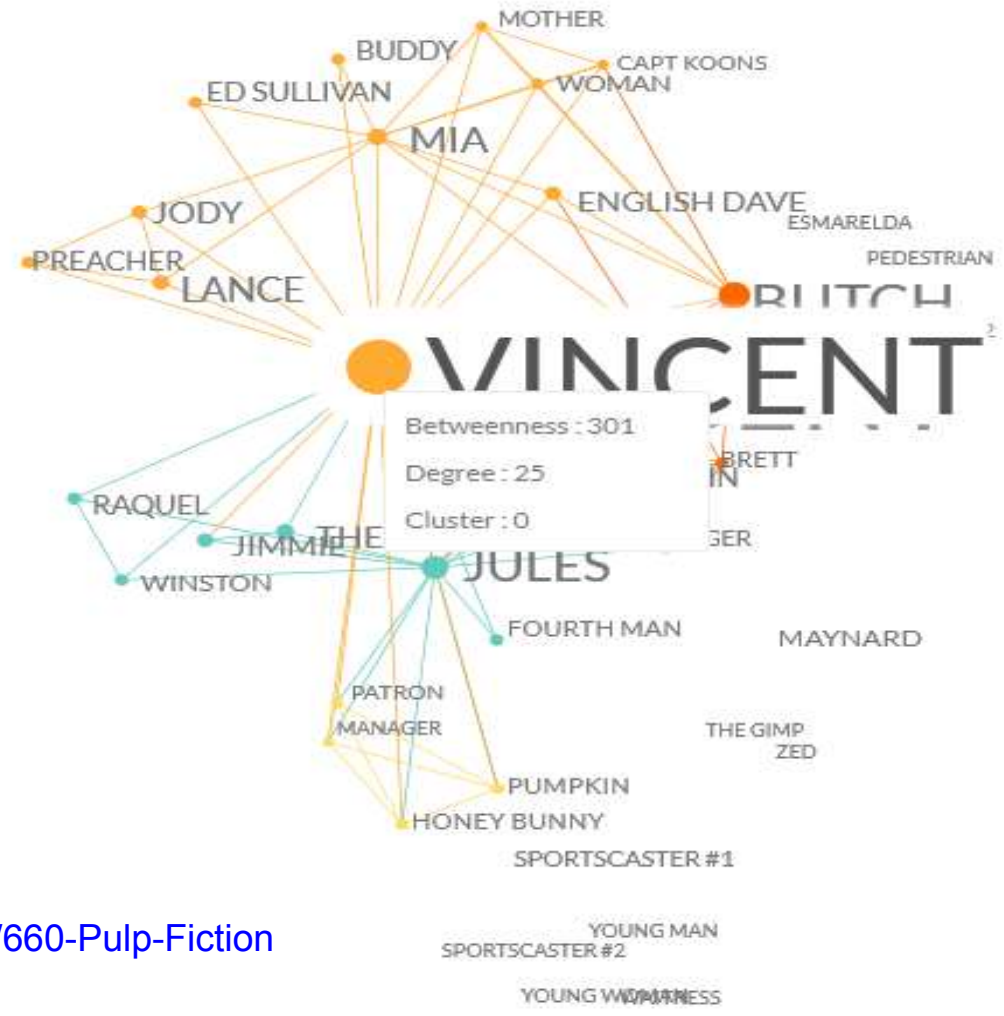


Movie Galaxies

Search for Movies

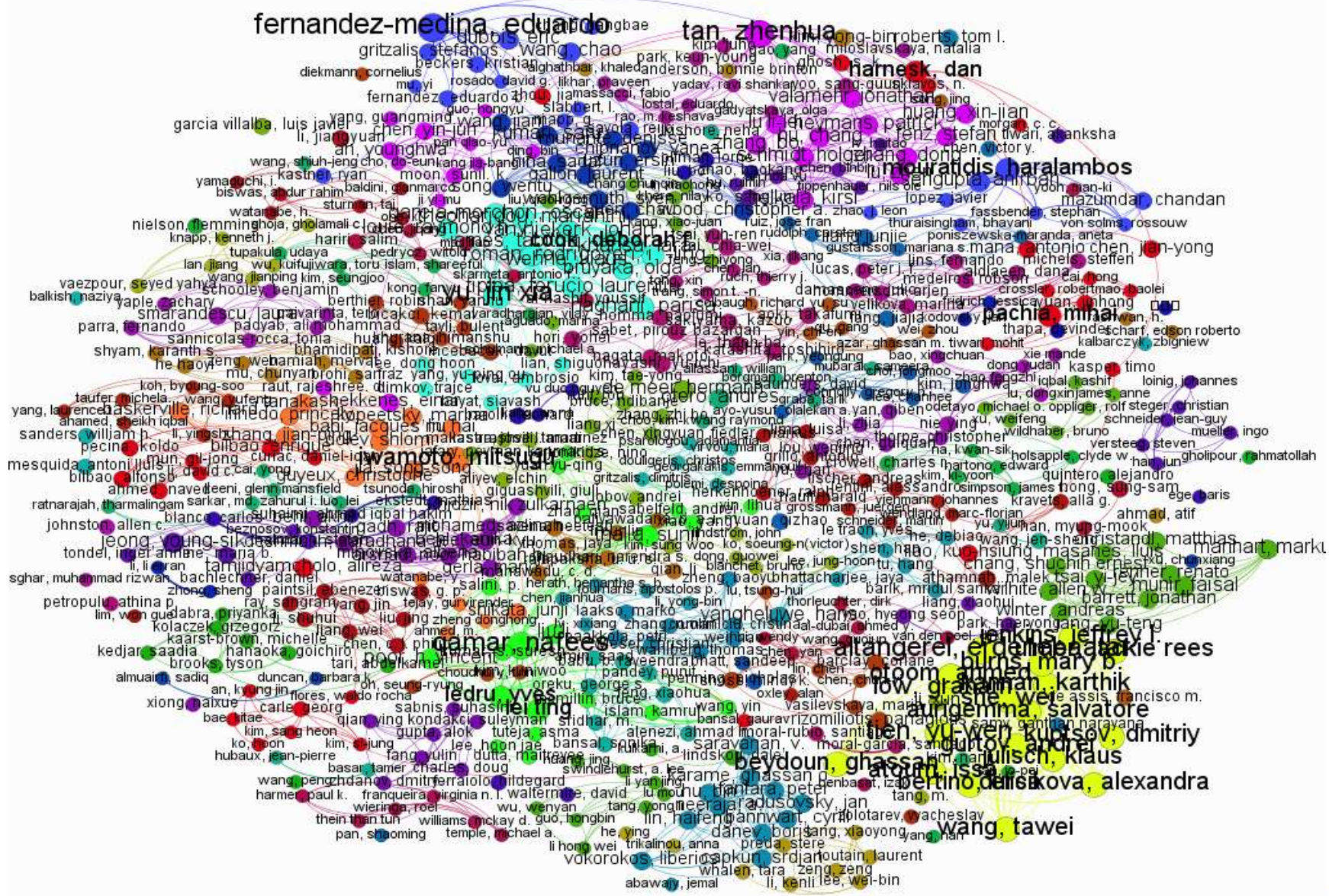
Recently Added | Most Clicked

PULP FICTION 1994



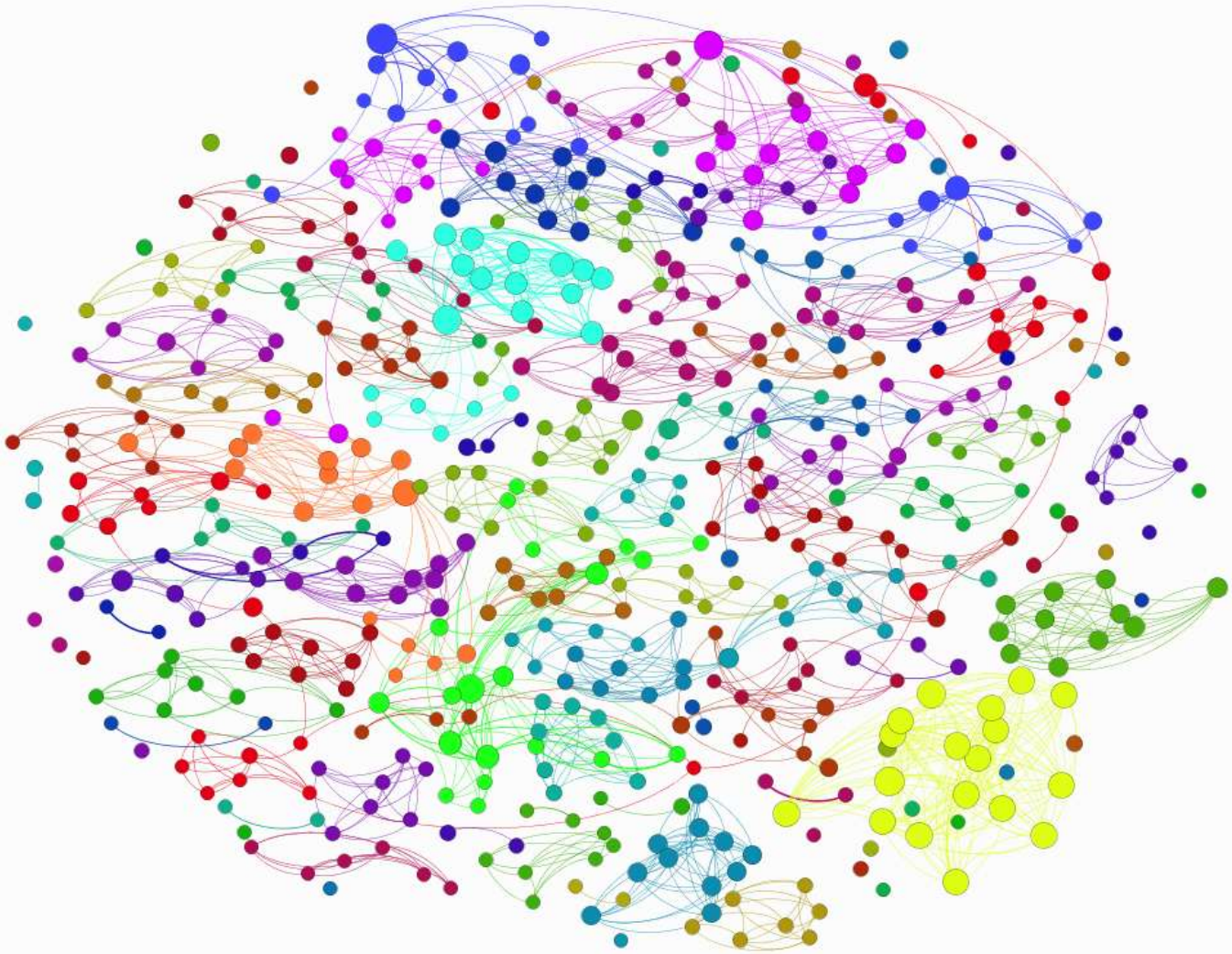
http://www.moviegalaxies.com/movies/660-Pulp-Fiction

Redes de Colaboração Científica



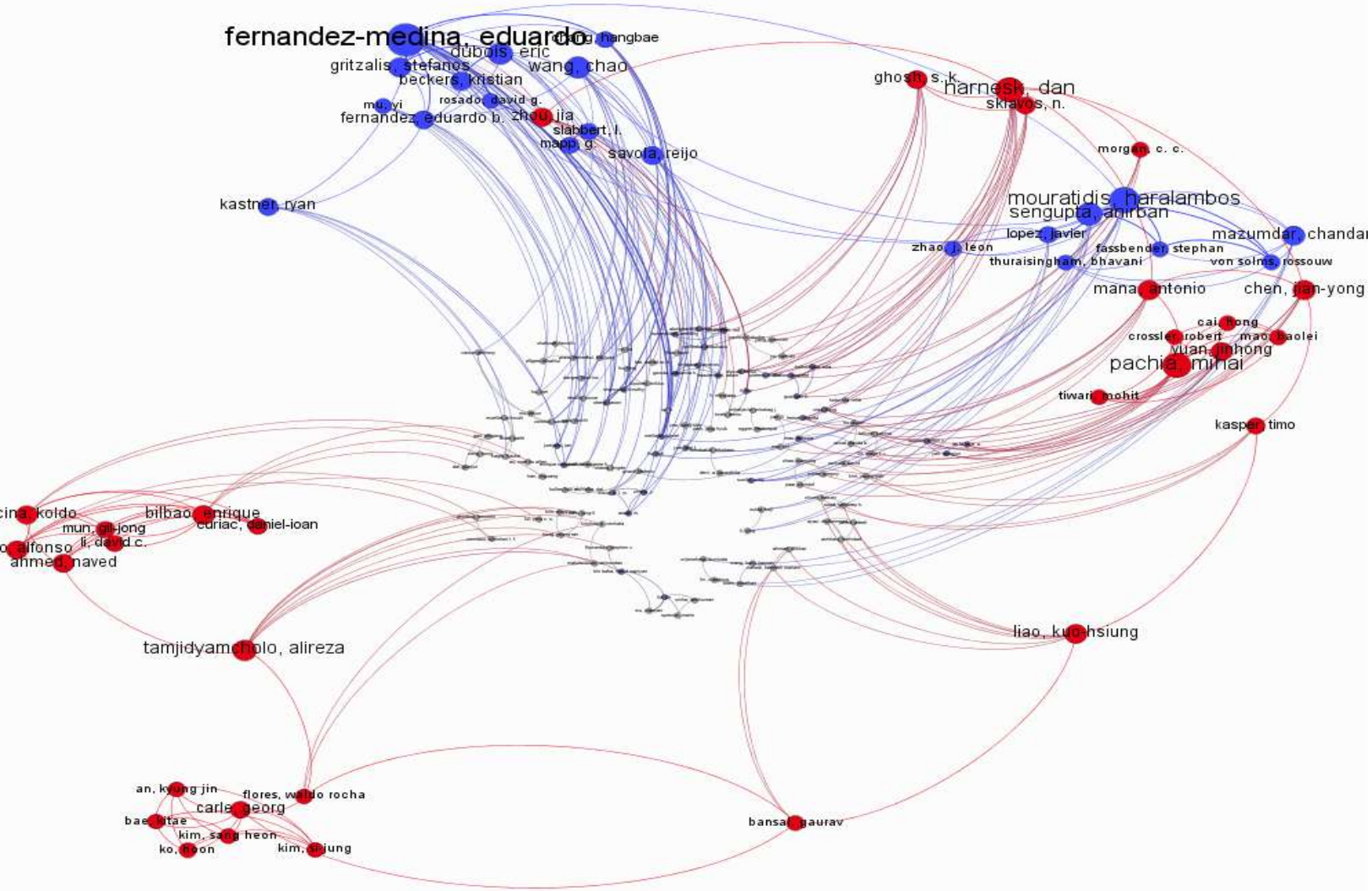
CTIRGov

Redes de Colaboração Científica



CTIRGov

Redes de Colaboração Científica



CTIRGov

Rede social

"Uma rede social consiste em um conjunto finito de atores e as relações definidas entre eles. (WASSERMAN E FAUST, 1994)"

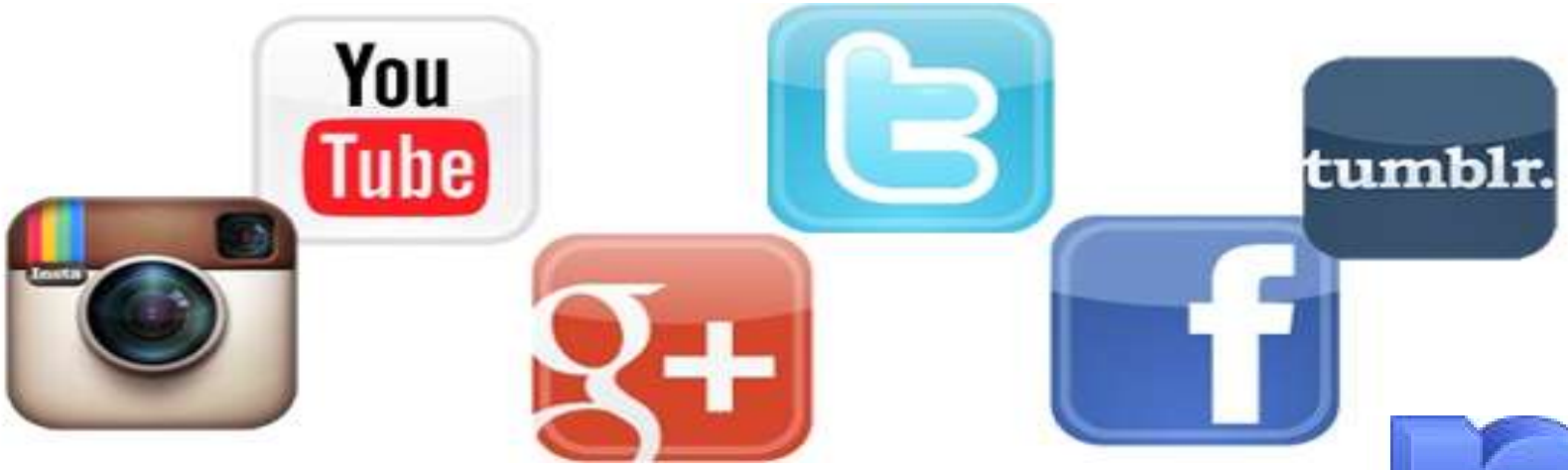
"Uma rede social representa um estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e propósitos comuns".

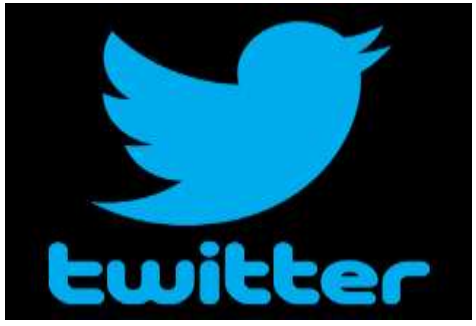
(FERREIRA, 2011)

redes sociais = mídias sociais?

mídias sociais:

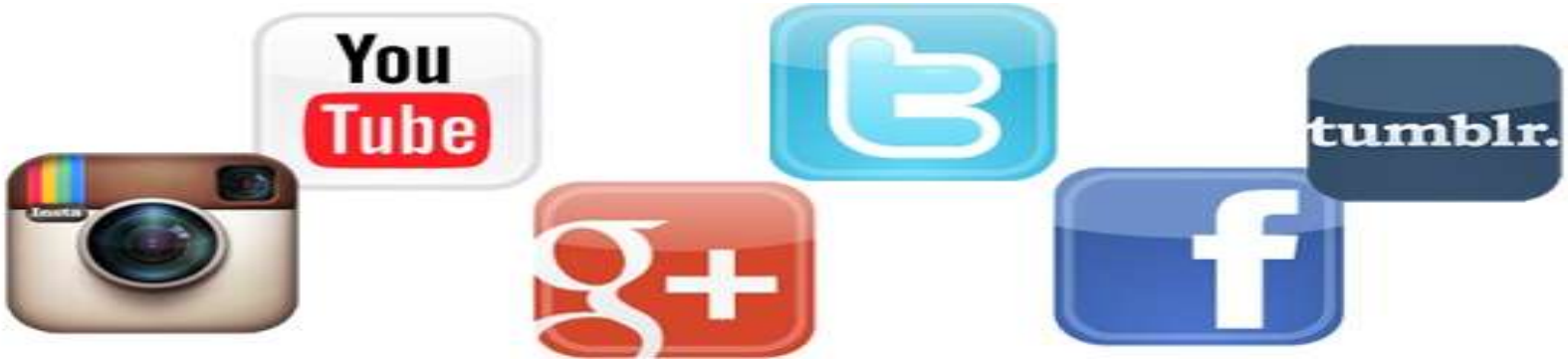
"Veículos que projetam conteúdos de forma descentralizada (Wikipédia)."



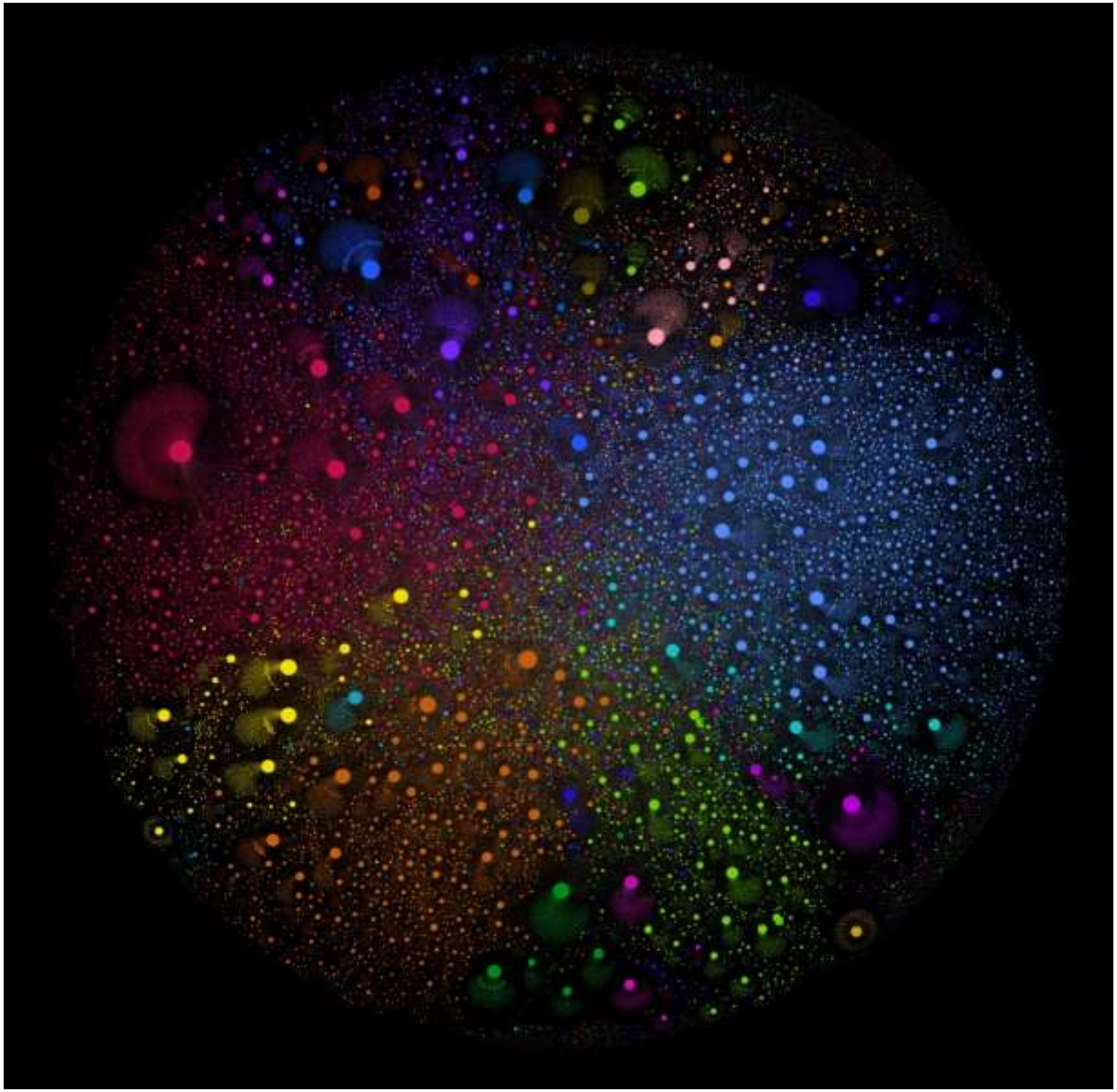


Ameaças nas redes sociais

Em anos recentes, grupos como o "Anonymous" tem alcançado enorme popularidade mundial, e têm sido responsáveis por grandes ataques contra empresas, instituições e governos (Paganini, 2013).



Manifestações de junho de 2013



Análise de fluxo realizada entre os dias 16 a 21 de junho de 2013.

Hashtag #ProtestoRJ

Dados extraídos do Twitter e visualizado no Gephi.

Grafo a partir da estatística de peso com aplicação de modularidade

Fonte: Medialab-UFRJ

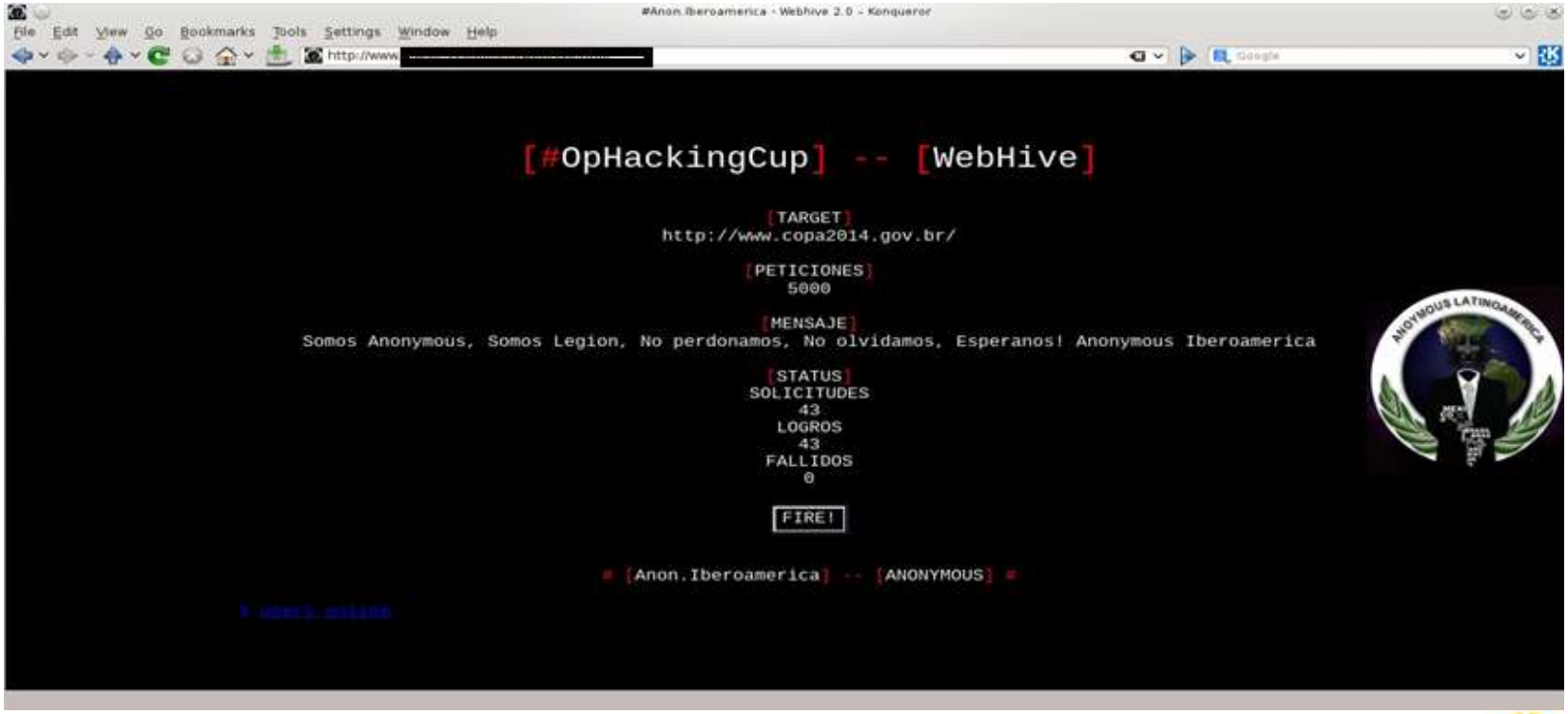
http://medialabufrj.net/2014/10/contagio-entre-as-redes-e-as-ruas-mapeando-o-protestorj-no-twitter

Copa do Mundo (Junho e Julho 2014)

INCIDENTES DE SEGURANÇA DE MAIOR RELEVÂNCIA

1. Ataques de Negação de Serviço:

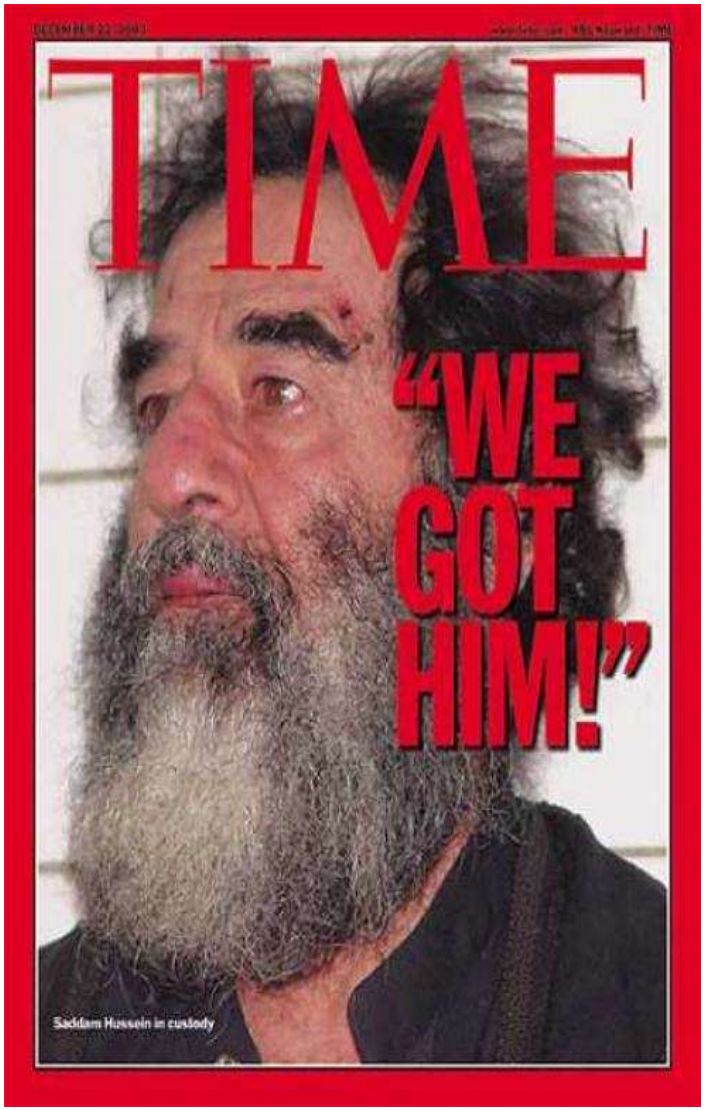
Os ataques de negação de serviço foram, em sua maior parte, detectados por meio de acompanhamento de redes sociais, o que permitiu identificar a hospedagem de diversas ferramentas para ataques de negação de serviço (DoS/DDoS) do tipo "LOIC" (*Low Orbit Ion Canon*).

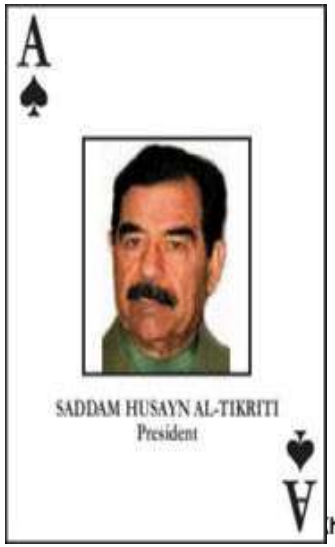


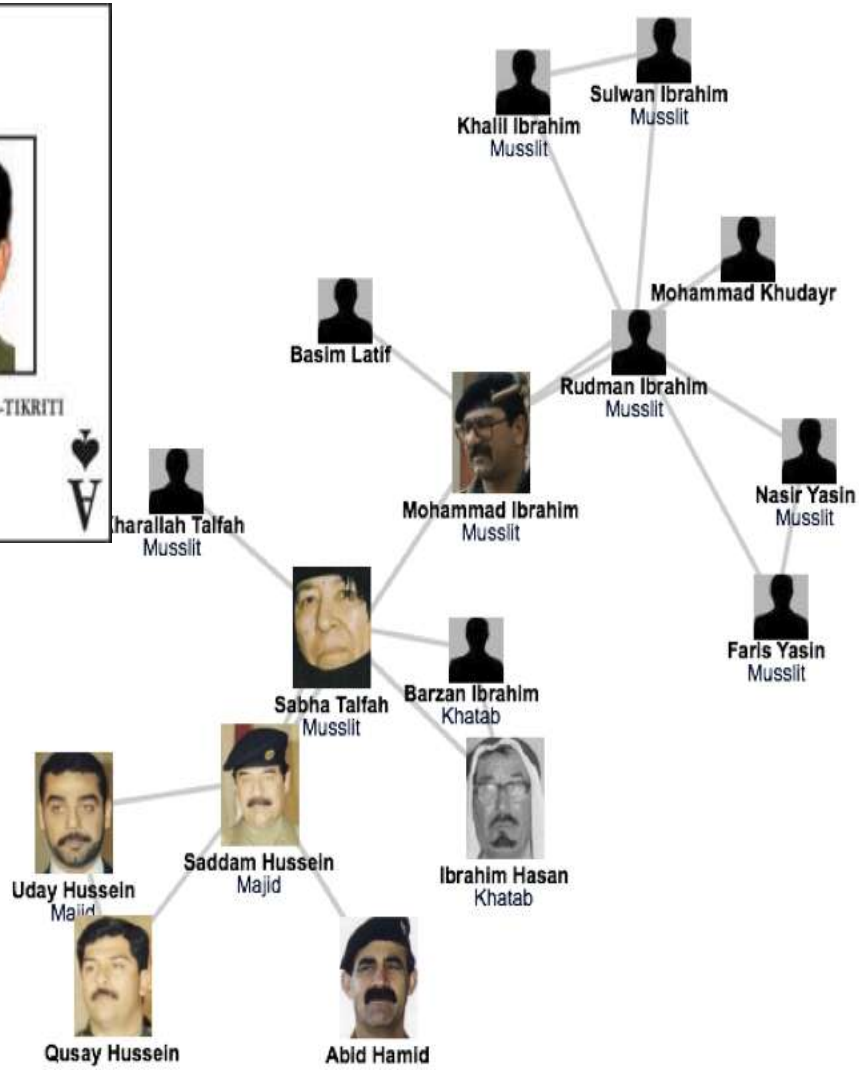
sítio comprometido hospedando LOIC contra o sítio copa2014.gov.br

CTIR Gov

A captura de Saddam Hussein







http://barabasilab.neu.edu/courses/phys5116

O poder das redes sociais

www.nytimes.com/interactive/2013/05/16/business/PHARMA.html?_r=4&

Pesquisar

Published: May 16, 2013

FACEBOOK TWITTER GOOGLE+ EMAIL SHARE

Drug Marketers Use Social Network Diagrams to Help Locate Influential Doctors

Consulting companies like Activate Networks create social network diagrams to help pharmaceutical marketers identify prescribing histories and relationships among doctors. Such diagrams can help marketers pinpoint highly connected physicians, the best potential targets for marketing. Related Article »

Doctors based in a Northeastern U.S. community who have prescribed, or are potential customers for, an oncology drug.

Each circle represents one doctor.

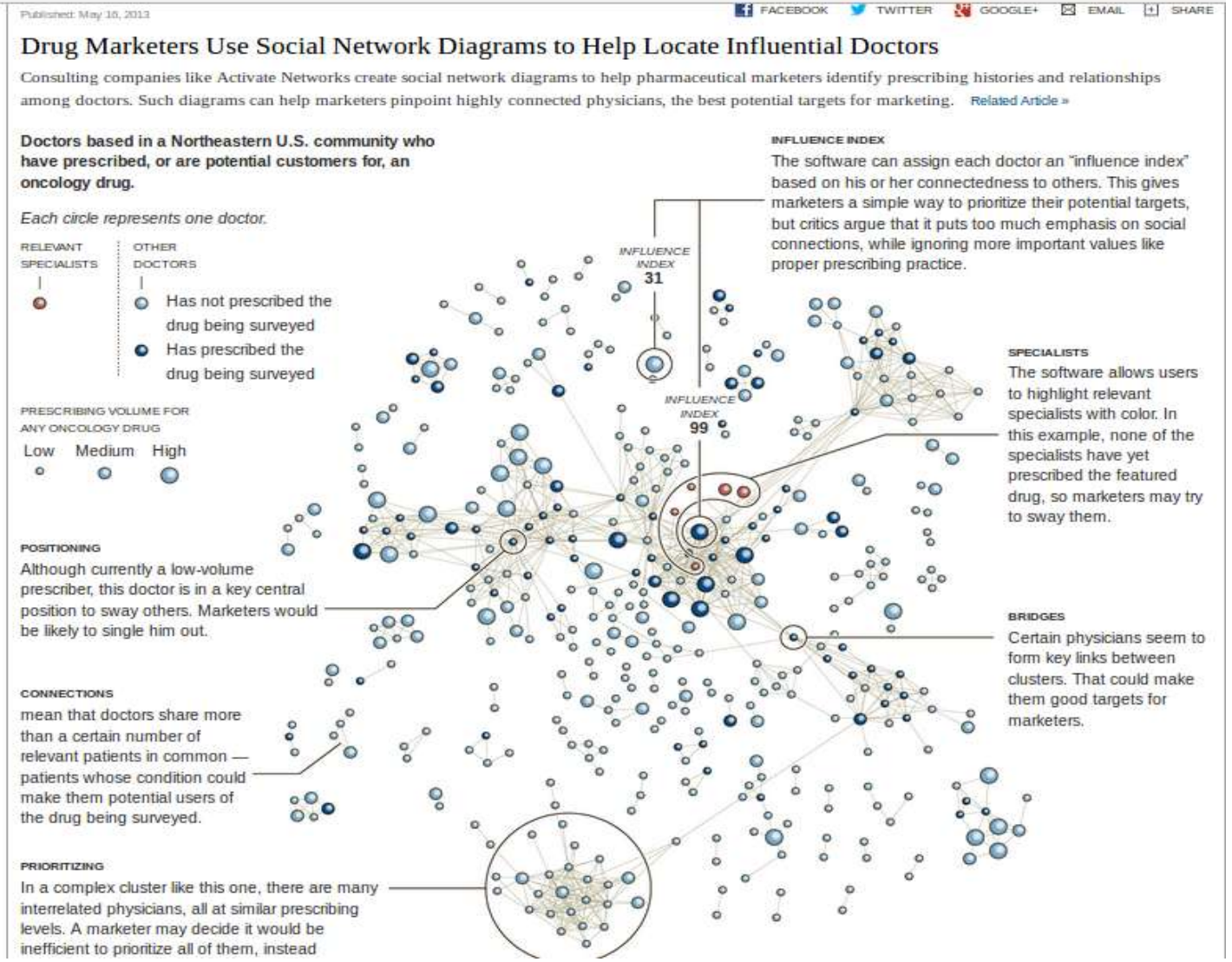
RELEVANT SPECIALISTS

OTHER DOCTORS

- Has not prescribed the drug being surveyed
- Has prescribed the drug being surveyed

PRESCRIBING VOLUME FOR ANY ONCOLOGY DRUG

Low Medium High



INFLUENCE INDEX
The software can assign each doctor an "influence index" based on his or her connectedness to others. This gives marketers a simple way to prioritize their potential targets, but critics argue that it puts too much emphasis on social connections, while ignoring more important values like proper prescribing practice.

SPECIALISTS
The software allows users to highlight relevant specialists with color. In this example, none of the specialists have yet prescribed the featured drug, so marketers may try to sway them.

BRIDGES
Certain physicians seem to form key links between clusters. That could make them good targets for marketers.

POSITIONING
Although currently a low-volume prescriber, this doctor is in a key central position to sway others. Marketers would be likely to single him out.

CONNECTIONS
mean that doctors share more than a certain number of relevant patients in common — patients whose condition could make them potential users of the drug being surveyed.

PRIORITIZING
In a complex cluster like this one, there are many interrelated physicians, all at similar prescribing levels. A marketer may decide it would be inefficient to prioritize all of them, instead

http://www.nytimes.com/interactive/2013/05/16/business/PHARMA.html?_r=4&

CTIRGov

Sumário

Agenda

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ **Grupos de Pesquisa**
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

CTIRGov

Grupos de Pesquisa - UnB/FioCruz

COLÓQUIO
de Análise de Redes
e Prospecção Tecnológica

de 26 a 28/08/2015

Busca...

Menu Lateral

- Palestrantes
- Apoio
- ComissãoOrganizadora
- Hospedagem
- Local do Evento
- Contato
- Networking

Conteúdo recente

- Networking
- Oficinas
- Apoio
- contato
- Sugestão de Hospedagem

Notícias

I Colóquio de Análise de Redes e Prospecção Tecnológica

22/5/2015

Participe do I Colóquio de Análise de Redes e Prospecção Tecnológica, em **Brasília, nos dias 26 a 28 de agosto de 2015**. Este

Medialab - UFRJ

medialabufrj.net/2012/09/oficina-grafos-de-redes-sociales-iniciacion-a-twapperkeeper-rstu

Pesquisar

MEDIALAB UFRJ

PROJETOS BLOG BIBLIOTECA AGENDA CONTATO EQUIPE PARCERIAS

OFICINA GRAFOS DE REDES SOCIAIS: INTRODUÇÃO À YOURTWAPPERKEEPER, RSTUDIO E GEPHI

PUBLICADO EM 9 DE SETEMBRO DE 2012 POR PABLO DE SOTO
CATEGORIAS: BLOG
TAGS: OFICINA, VISUALIZAÇÃO DE DADOS

Pesquisar

TÓPICOS RECENTES

- Olho_Máquina_Mundo
- A Vida Secreta dos Objetos: Ecologias da Mídia
- III Simpósio Internacional LAVITS _ VIDEOS ONLINE!!!
- Sapiens construiram drones na ECO UFRJ
- #DRONEHACKADEMY: COMO E POR QUE PROTEGER-SE DOS VEÍCULOS AÉREOS NÃO TRIPULADOS

TAGS

#LutasGlobais arquivo audiovisual cartografia

CTIRGov

LABIC


www.labic.net
Pesquisar
Labic
Laboratório de estudos sobre
Imagem e Cibercultura
LABIC
BLOG
PUBLICAÇÕES
CARTOGRAFIAS
CONTATO
marisa_lobo
marcelotas
pastormalafaia
O jornalismo nas redes sociais:
autoridade sem centralidade
A grande reconversão jornalística tem sido feita por repórter profissionais e amadores que entram nas manifestações e, de dentro dela, relatam. No Brasil, essa metamorfose é notável com os “ninjas” e a força de seus dispositivos multimídia in streaming.

Convênio do LABIC com a SDH/PR

www.sdh.gov.br/noticias/2014/novembro/crimes-virtuais-matam-afirma-ministra-du

Pesquisar

Departamento da Polícia Federal, Ministério Público Federal, Ordem dos Advogados do Brasil e Colégio Nacional dos Defensores Públicos Gerais (**CONDEGE**).

Além do Grupo de Trabalho, a **SDH/PR** firmou com a Universidade Federal do Espírito Santo (UFES) um Termo de Execução Descentralizada por intermédio do qual o Laboratório de Estudos em Imagem e Cibercultura (LABIC) – referência internacional em pesquisas sobre redes sociais - auxiliará a Secretaria no mapeamento tanto de redes de apologia ao crime quanto de redes de defesa dos direitos humanos.

Pelo Termo de Execução, o LABIC também desenvolverá um aplicativo para que a Secretaria possa acompanhar a atuação destas redes, elaborando estratégias de comunicação específicas para cada uma delas, além de capacitar a equipe da Secretaria no uso do deste aplicativo.

Assessoria de Comunicação Social com Agência Brasil

www.sdh.gov.br

https://www.facebook.com/direitoshumanosbrasil

CTIR Gov

Sumário

oglobo.globo.com/sociedade/governo-vai-usar-aplicativo-para-monitorar-crimes-cc

Pesquisar

O GLOBO MENU SOCIEDADE

Página "O racismo começa quando" reúne cerca de 30 mil "curtidas" e está sendo investigada pela Polícia Civil - **Reprodução / Facebook**

BRASÍLIA - A Secretaria de Direitos Humanos da Presidência da República criou nesta quinta-feira grupo de trabalho para mapear e monitorar crimes contra os direitos humanos nas redes sociais. O grupo será formado por representantes de diferentes ministérios, inclusive da Polícia Federal, e utilizará informações fornecidas pelo Laboratório de Estudos em Imagem e Cibercultura (Labic) da Universidade Federal do Espírito Santo. O laboratório desenvolveu um aplicativo capaz de monitorar em tempo real milhões de mensagens postadas em redes como Facebook, Twitter, Instagram, Youtube e Flickr.

— Não vamos substituir o trabalho de ninguém. O que vamos fazer é articular e interagir com os ministérios que atuam nessas áreas, agilizando ações contra aquilo que se configurar como ato criminoso - disse Ideli

Projeto Interagentes

interagentes.net/?p=583

Pesquisar

#interagentes

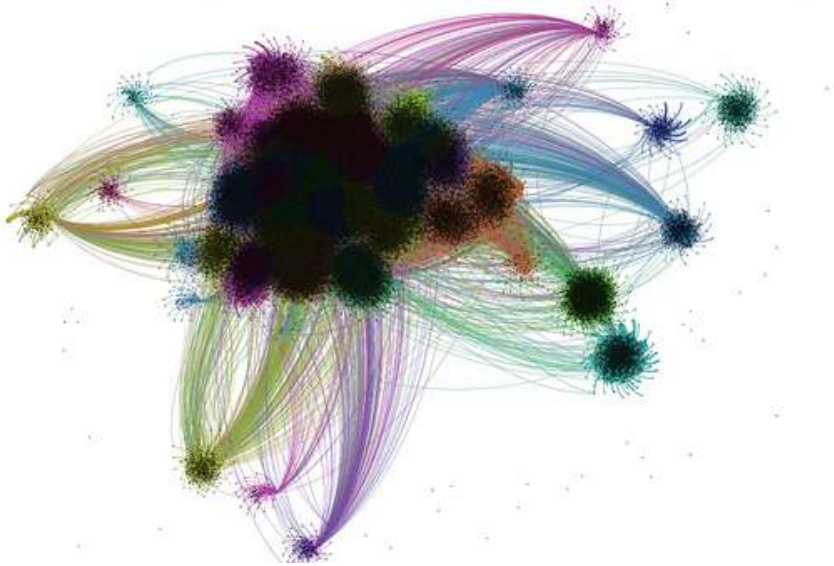
Comunicação Digital e Ações em Rede

Artigos Sobre Contato

Prévia de dados: mobilizações de 16 de agosto

Date: 14 de agosto de 2015 Posted by interagentes No Comments Category: Sem categoria

To search type and hit Enter...



CTIRGov

Sumário

Agenda

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ **Algumas ferramentas**
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ Conclusões

CTIRGov

Análise de Redes Sociais (ARS)

"Metodologia para detectar e interpretar padrões de vínculos e/ou relações sociais entre atores. (NOOY. et al, 2005)".

- Ferramentas de Coleta:
  - YourTwapperKeeper, NodeXL, ...

- Ferramentas de Tratamentos de Dados:
  - R Language, PAJEK,....

- Ferramentas de Inspeção visual
  - VosViewer; Gephi; ORA; UCINET, NodeXL , TAGs,...

CTIRGov

Análise de Redes Sociais (ARS)

Exemplos de Clawlers (material do Labic)

Flocker

Webapp que age como estruturador de redes de *retweets* em tempo real. Permite exportar o grafo criado para GEXF, PNG e SVG.

Licença: gratuita.

Site: www.flocker.outliers.es

Netvizz

Aplicativo do Facebook de fácil utilização que possibilita extrair as redes de amigos, páginas e grupos a que o usuário principal está conectado.

Licença: gratuita.

Site: www.apps.facebook.com/netvizz

NodeXL

Extensão para o Microsoft Excel que permite extrair dados de redes como Facebook e Twitter e posterior manipulação no programa ou exportação para Gephi.

Licença: gratuita.

Site: www.nodexl.codeplex.com

Plugin Social Network Importer: www.socialnetimporter.codeplex.com

Topsy

Permite extrair dados da rede do Twitter. Pela parceria que tem com a rede social, é o único que não possui limite de tempo de publicação do *tweet* nem limite de requisições ao servidor. É o sucessor do YourTwapperKeeper.

Licença: versão limitada gratuita e profissional paga.

Site: www.topsy.com

YourTwapperKeeper

Permite a configuração de diferentes *keywords* para monitoração, captura e armazenamento de *tweets* em tempo real. Necessita de instalação.

Licença: código aberto.

Site: www.github.com/540co/yourTwapperKeeper

https://db.tt/z00cve04

CASOS Project

casos.cs.cmu.edu

Pesquisar

Home | Institute for Software Research | CMU Computer Science

Search CASOS:

Navigation: Home >

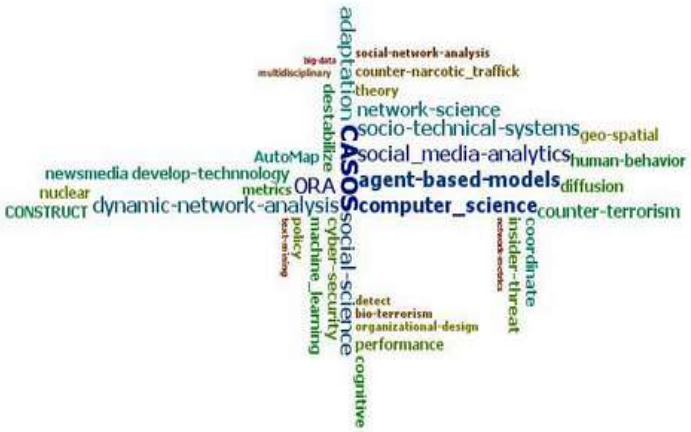
CASOS

- Home
- Mission
- People
- News
- Education
- Tools, Models & Data
- Events
- Projects
- Networks & Terrorism
- Publications & Search
- Community
- Links
- Contact Us

Welcome to Center for Computational Analysis of Social and Organizational Systems (CASOS)!

Addressing complex real world issues through a combined social-science & computer-science approach, using advanced techniques from network science, text-mining, and agent-based modeling.

- Leader in network dynamics and linking social networks to other data - geo-spatial, knowledge, tasks etc.
- Leading analytic tools for network analysis - ORA, AutoMap, Construct
- University wide center with faculty and students in multiple departments
- Multi-disciplinary research - working with Academia, Industry, Government
- Applications related to Law Enforcement, Counter-terrorism, Health, Nuclear Deterrence, Cyber-Security, Social Change, Organizational Design, Insider Threat



ORA

Analyze statistics, social network analysis (SNA), dynamic network analysis (DNA), link analysis software.

Learn more

Papers

Current Projects

- Social Media, News and the Arab Spring
- Tracking Covert Groups on Twitter
- Testing social theory with FourSquare data
- Event Detection from Twitter using Hierarchical Bayesian Models
- Measuring Network Stability and Fit
- Twitter in Indonesia, for Tsunami Planning & Alerts

Recent News

August 3-5, 2015 - CMU CASOS hosts ONR 2015 Disaster Tools Technical Exchange This international meeting brings together university, non-government organizations, and various government organizations concerned with developing

CTIRGov

CASOS Project

Center for Computacional Analysis of Social and Organizational Systems (CASOS)

Home | Institute for Software Research | CMU Computer Scienc

Navigation: Home > Projects >

- Home
- Mission
- People
- News
- Education
- Tools, Models & Data
- Events
- Projects
- Networks & Terrorism
- Publications & Search
- Community
- Links
- Contact Us

Tracking Covert Groups on Twitter - Overview

Overview | People | Collaborators | Sponsors | Publications | Tools

Overview

Many covert and terror groups have a strong presence in social media. ISIS, in particular, is well known for its use of social media. Twitter is one of the dominant media used. Members of ISIS, ISIS sympathizers, and those watching ISIS, both women and men, send tweets about concerns, activities, and attitudes. Can such information, can such networks of people and topics, be used to identify the members of the group and potential converts?

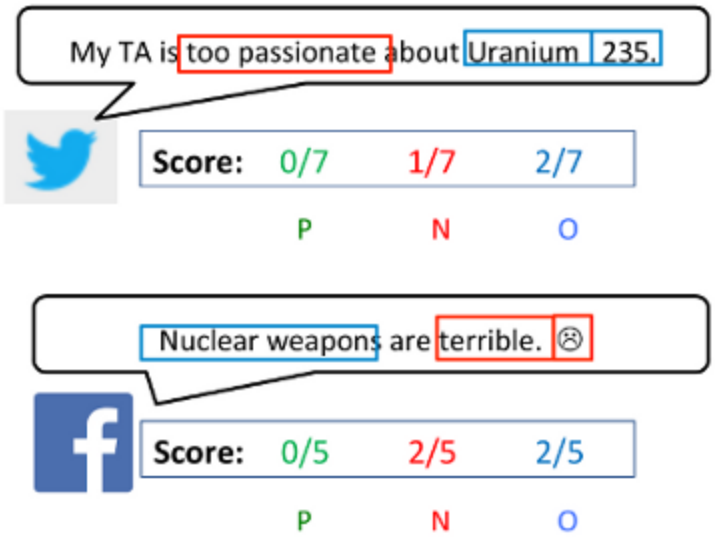
The ability to use social media and open source public information to identify covert networks and potential recruits could provide critical new capabilities to governments and security forces. However, detecting this large network from publically available data is a challenge. In this project we are investigating search techniques utilizing the open source public Twitter under the creative commons license to identify and analyze the ISIS propaganda network.

http://www.casos.cs.cmu.edu/projects/project.php?ID=86&Name=Tracking%20Covert%20Groups%20on%20Twitter

CTIRGov

CASOS / ORA - CMU

CASOS Gallery



	People	Knowledge	Tasks
People	Social Network Who knows who	Knowledge Network Who knows what	Assignment Network Who does what
Knowledge		Information Network What informs what	Needs Network What knowledge is needed to do the task
Tasks			Precedence Network Which task must be done before which

*ORA can be applied both within a traditional organization or on covert networks.

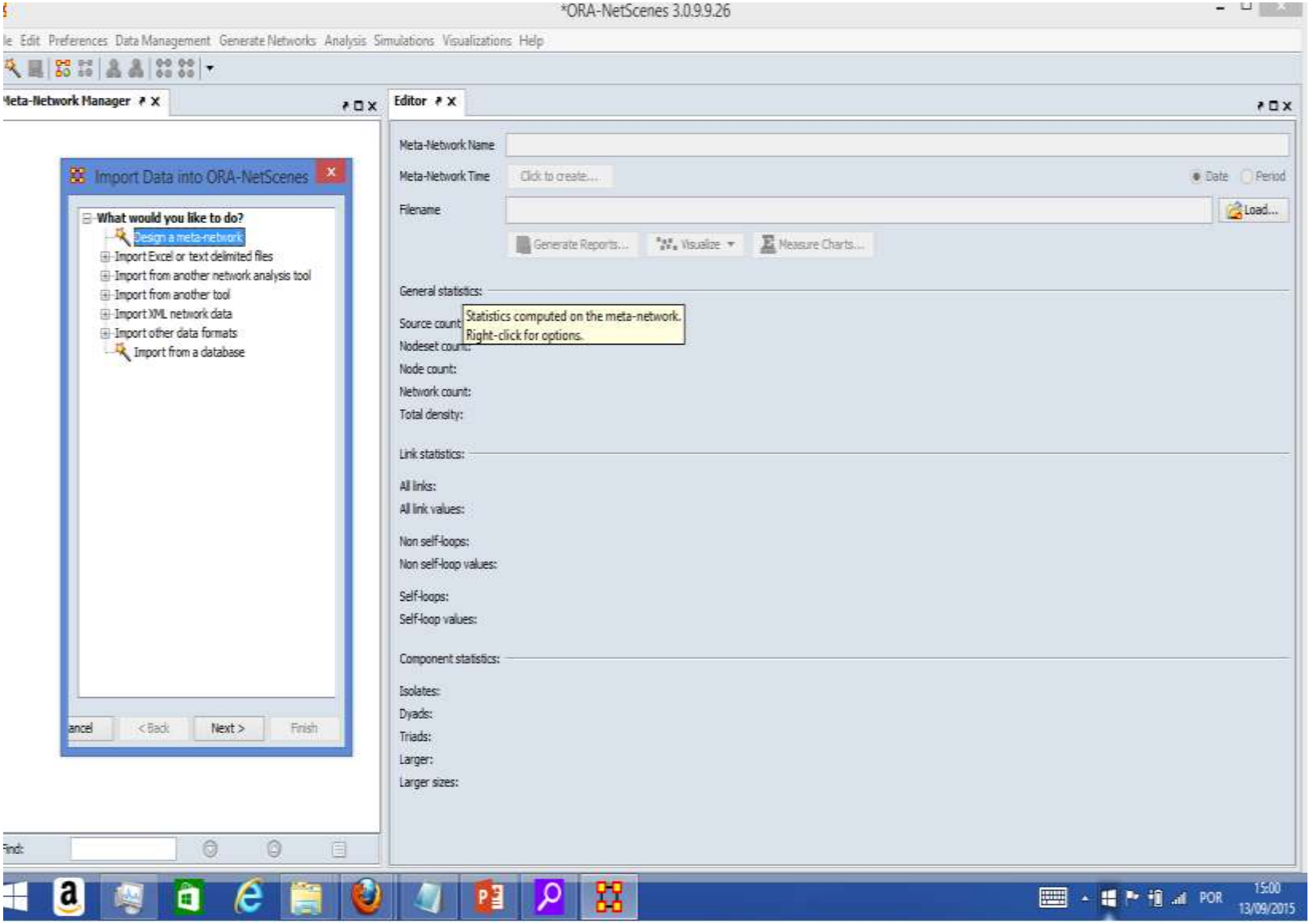
ORA Google Group

The ORA Google Group provides a forum for questions, collaborations, and information related to CASOS tools. Please visit this link for instructions on

http://www.casos.cs.cmu.edu/projects/ora/

CTIRGov

ORA Software



Arizona State University's TweetTracker

tweettracker.fulton.asu.edu

TweetTracker.

There are over a billion tweets sent to Twitter every week.
TweetTracker is a **powerful** tool from Arizona State University that can help you **track**, **analyze**, and **understand** activity on Twitter.

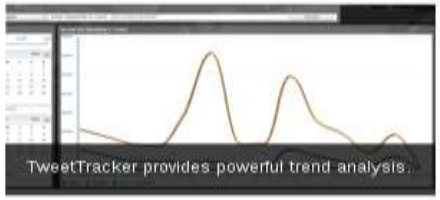
Disaster Preparedness

Humanity Road Inc. uses TweetTracker to monitor emerging disasters, and Quicknets partnered with us to test their system in a disaster simulation game on the Arizona State University Campus.

Cutting-Edge Research

ARTIS Research and University of Michigan used data collected through TweetTracker to analyze the factors responsible for Arab Spring, and Carnegie Mellon University and the School of Social Transformation at ASU use TweetTracker for their research as well.

TweetTracker has analyzed over 2,385,437,039 tweets!



Step 1. Track
TweetTracker collects tweets according to hash

Step 2. Analyze
TweetTracker allows you to compare activity across

Step 3. Understand
TweetTracker provides visualizations across a

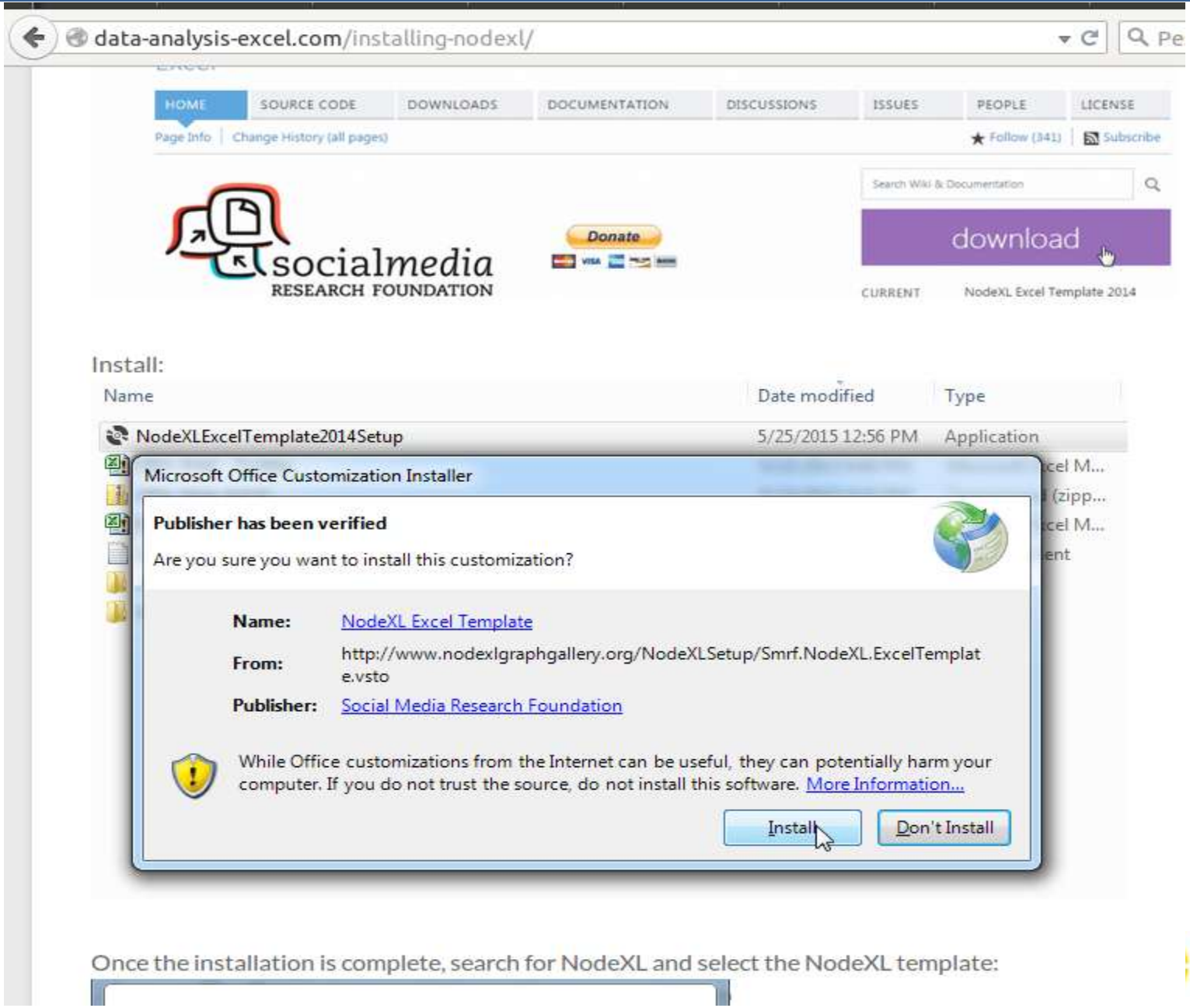
http://tweettracker.fulton.asu.edu/

CTIRGov

COSMOS

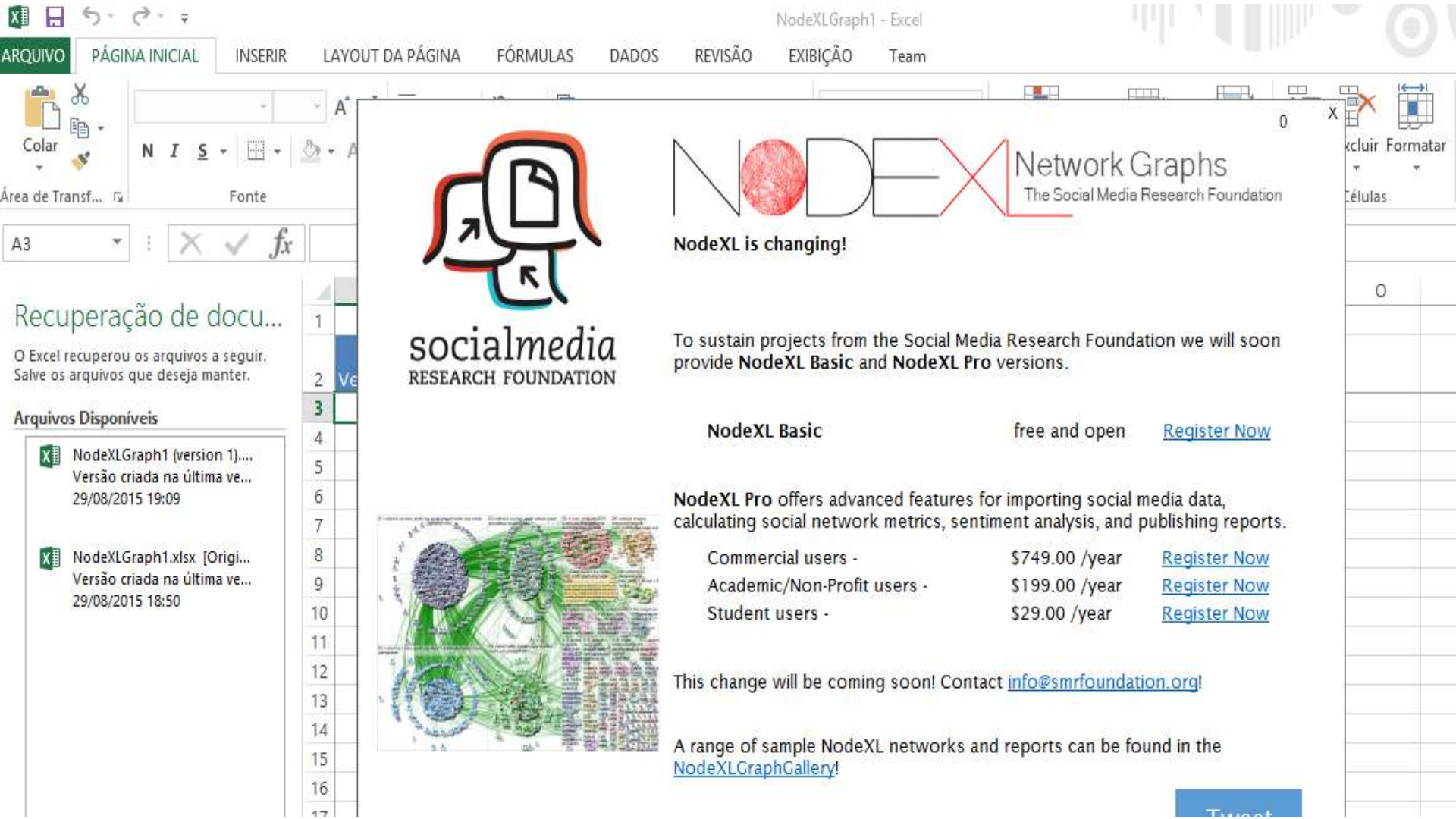
CTIRGov

NodeXL

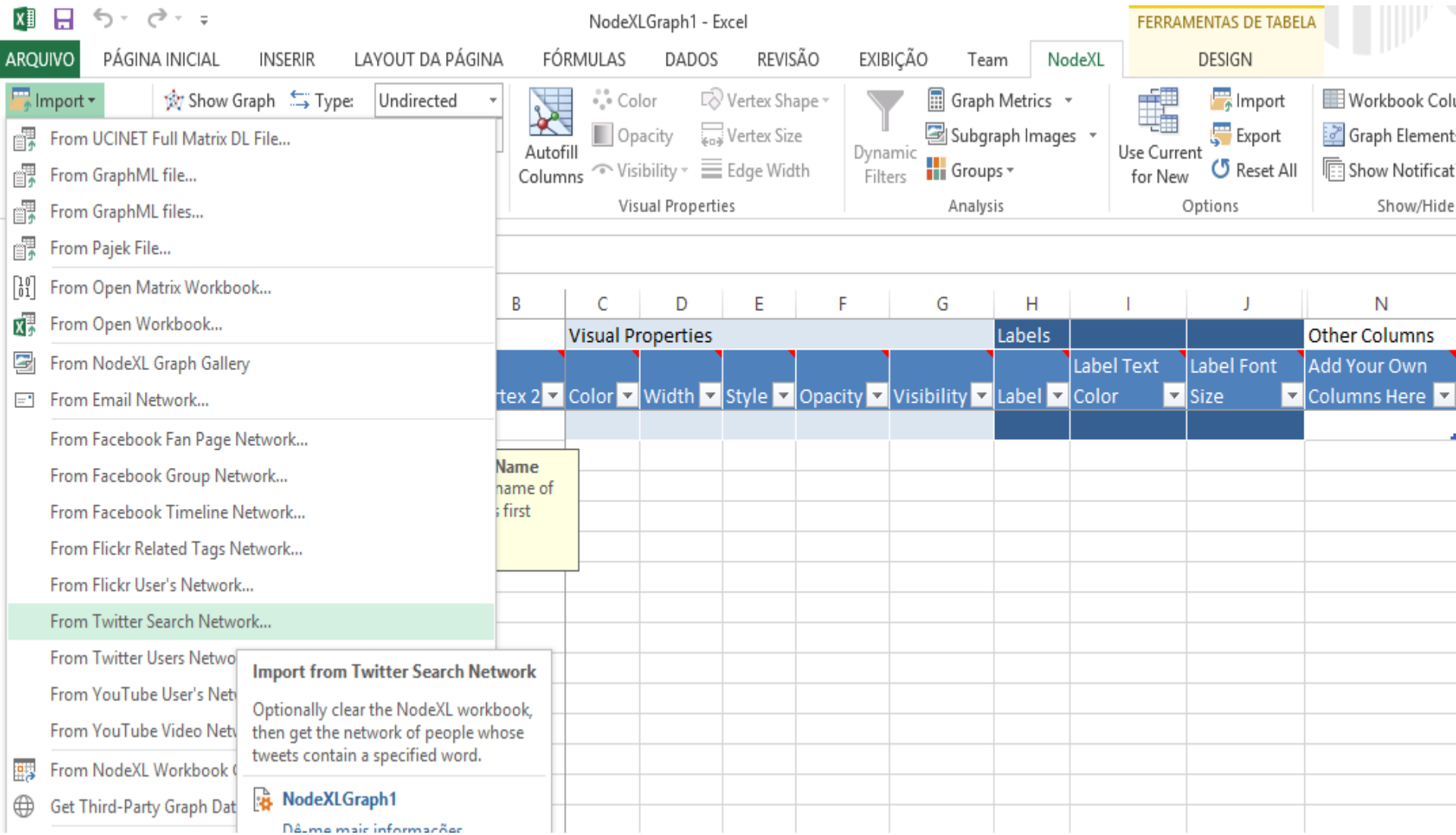


CTIRGov

NodeXL


NodeXLGraph1 - Excel
ARQUIVO
PÁGINA INICIAL
INSERIR
LAYOUT DA PÁGINA
FÓRMULAS
DADOS
REVISÃO
EXIBIÇÃO
Team
Colar
Área de Transf...
Fonte
A3
Recuperação de docu...
O Excel recuperou os arquivos a seguir.
Salve os arquivos que deseja manter.
Arquivos Disponíveis
NodeXLGraph1 (version 1)....
Versão criada na última ve...
29/08/2015 19:09
NodeXLGraph1.xlsx [Origi...
Versão criada na última ve...
29/08/2015 18:50
socialmedia
RESEARCH FOUNDATION
NODEXL
Network Graphs
The Social Media Research Foundation
NodeXL is changing!
To sustain projects from the Social Media Research Foundation we will soon provide NodeXL Basic and NodeXL Pro versions.
NodeXL Basic
free and open
Register Now
NodeXL Pro offers advanced features for importing social media data, calculating social network metrics, sentiment analysis, and publishing reports.
Commercial users -
$749.00 /year
Register Now
Academic/Non-Profit users -
$199.00 /year
Register Now
Student users -
$29.00 /year
Register Now
This change will be coming soon! Contact info@smrfoundation.org!
A range of sample NodeXL networks and reports can be found in the NodeXLGraphGallery!

NodeXL



CTIRGov

TAGS

TAGS

Need a Twitter Archiving Google Sheet?

TAGS is a free Google Sheet template which lets you setup and run automated collection of search results from Twitter.

Get TAGS

Tweet

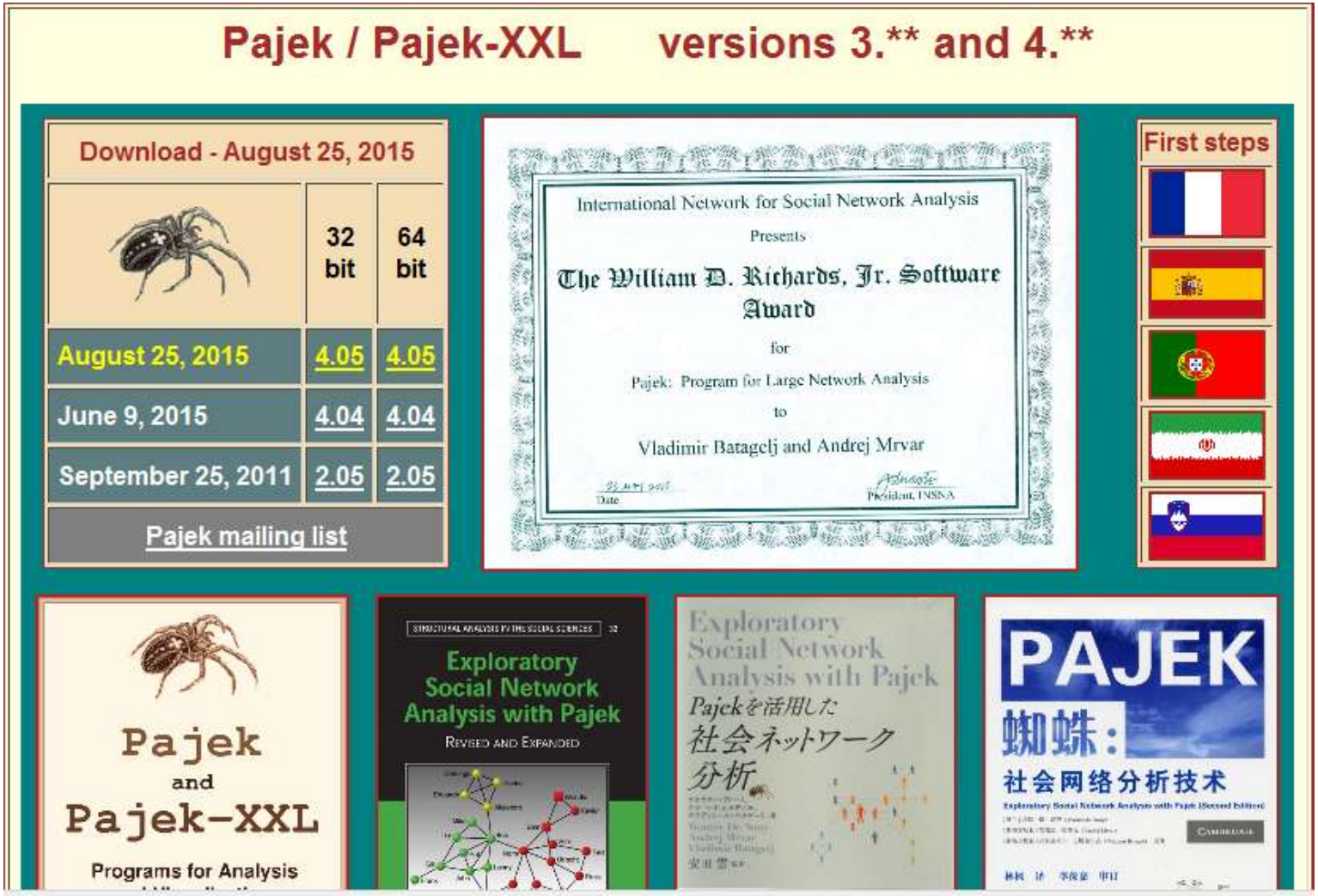
G+1

https://tags.hawksey.info/

CTIRGov

Ferramenta para manipulação dos dados

1ª Ferramenta para rede de grande volume de dados



http://mrvar.fdv.uni-lj.si/pajek/

Ferramenta para manipulação dos dados

The R Project for Statistical Computing

```
dens <- density(data, n = npts)
    dx <- dens$x
    dy <- dens$y
    if(add == TRUE)
        plot(0., 0                    main
             ylab
    if(orientati          ==
      dx2 <- (dx          min
        x[1.]
      dy2 <- (dx - min
        y[1.]
      seqbelow <- rep(y[1.], length(dx))
```

https://www.r-project.org/

CTIRGov

Ferramentas de visualização

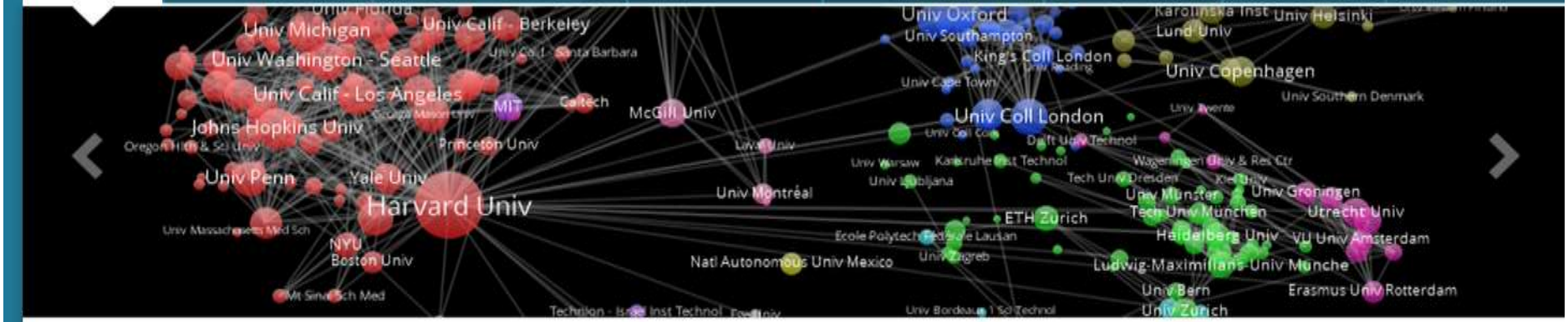
www.vosviewer.com/Home

VOSviewer

Visualizing scientific landscapes

Leiden University | CWTS | CWTS B.V. | Other CWTS sites

Home | Features | Getting Started | Download | Publications | Products | Contact



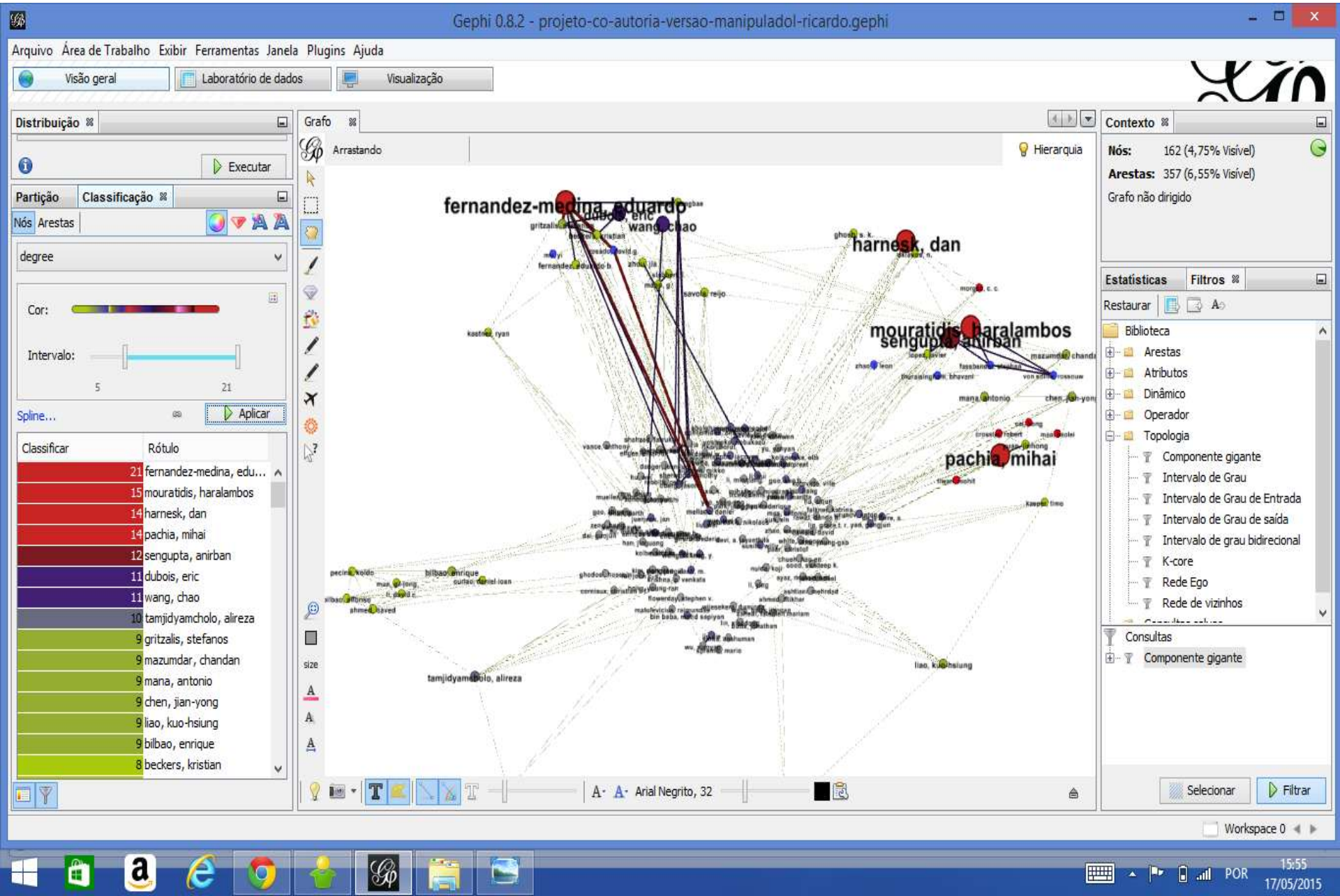
Welcome to VOSviewer

VOSviewer is a software tool for constructing and visualizing bibliometric networks. These networks may for instance include journals, researchers, or individual publications, and they can be constructed based on co-citation, bibliographic coupling, or co-authorship relations. VOSviewer also offers text mining functionality that can be used to construct and visualize co-occurrence networks of important terms extracted from a body of scientific literature.

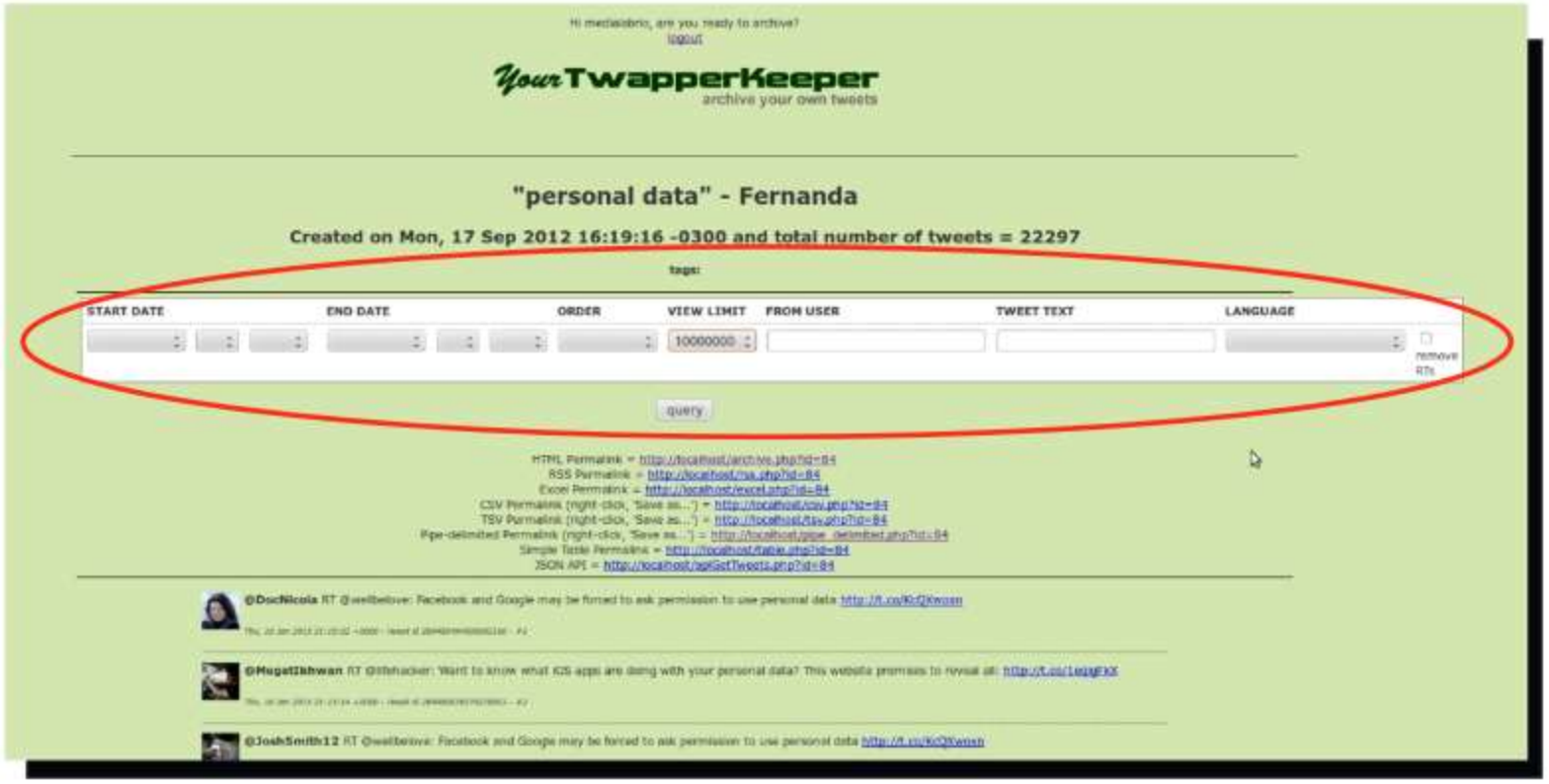
http://www.vosviewer.com/Home

CTIRGov

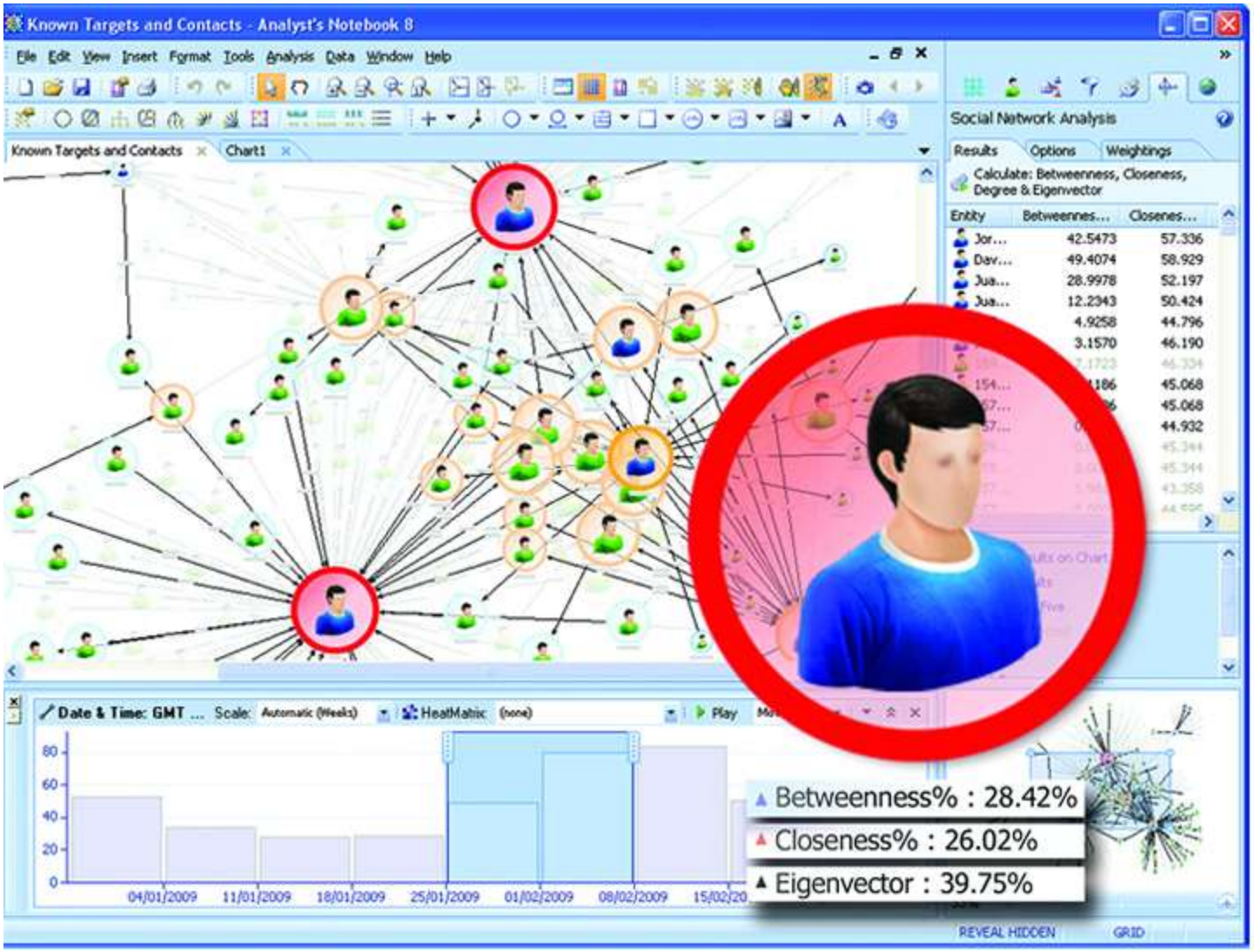
Ferramentas de visualização



YourTwapperkeeper

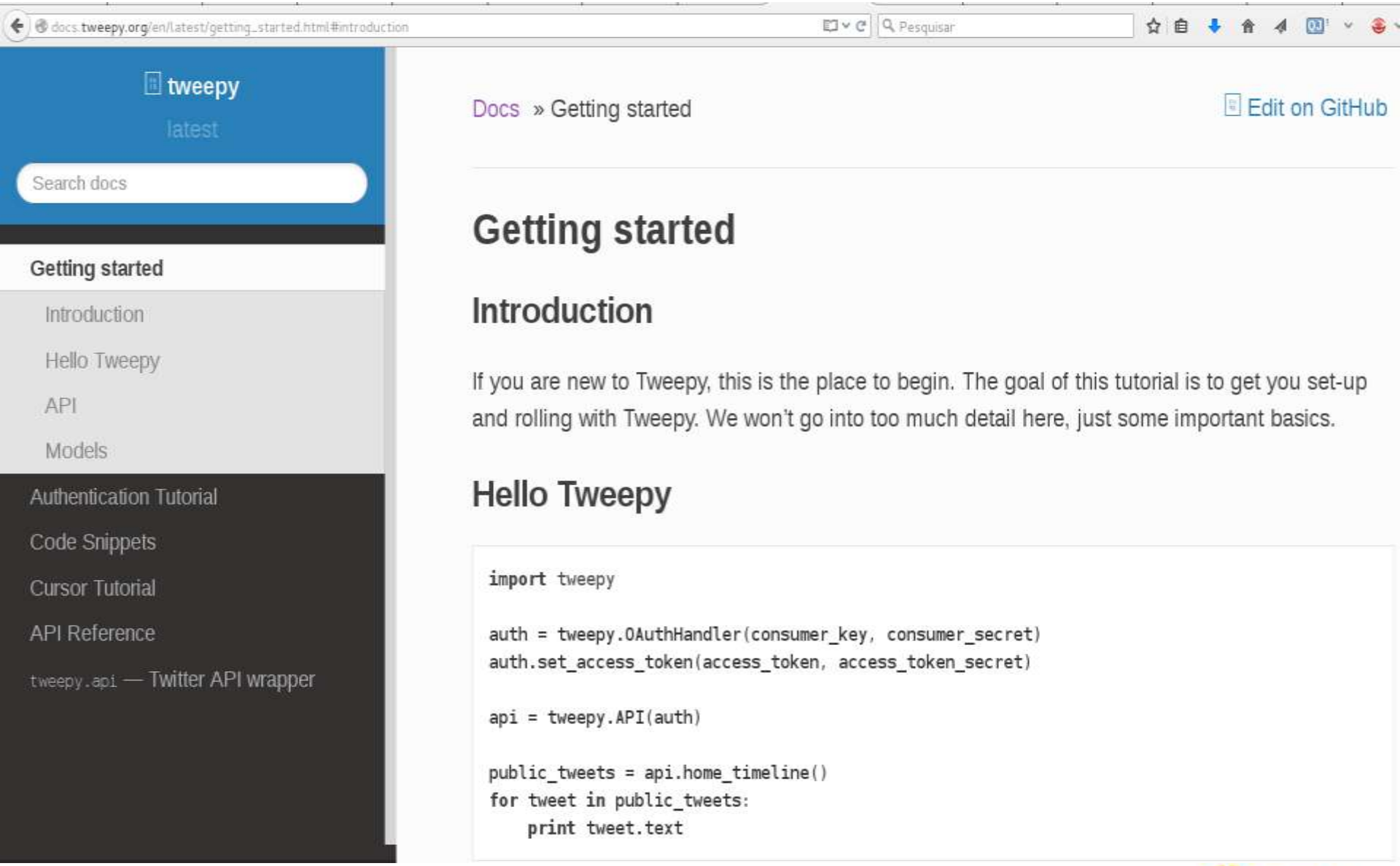


IBM i2 Analyst's Notebook

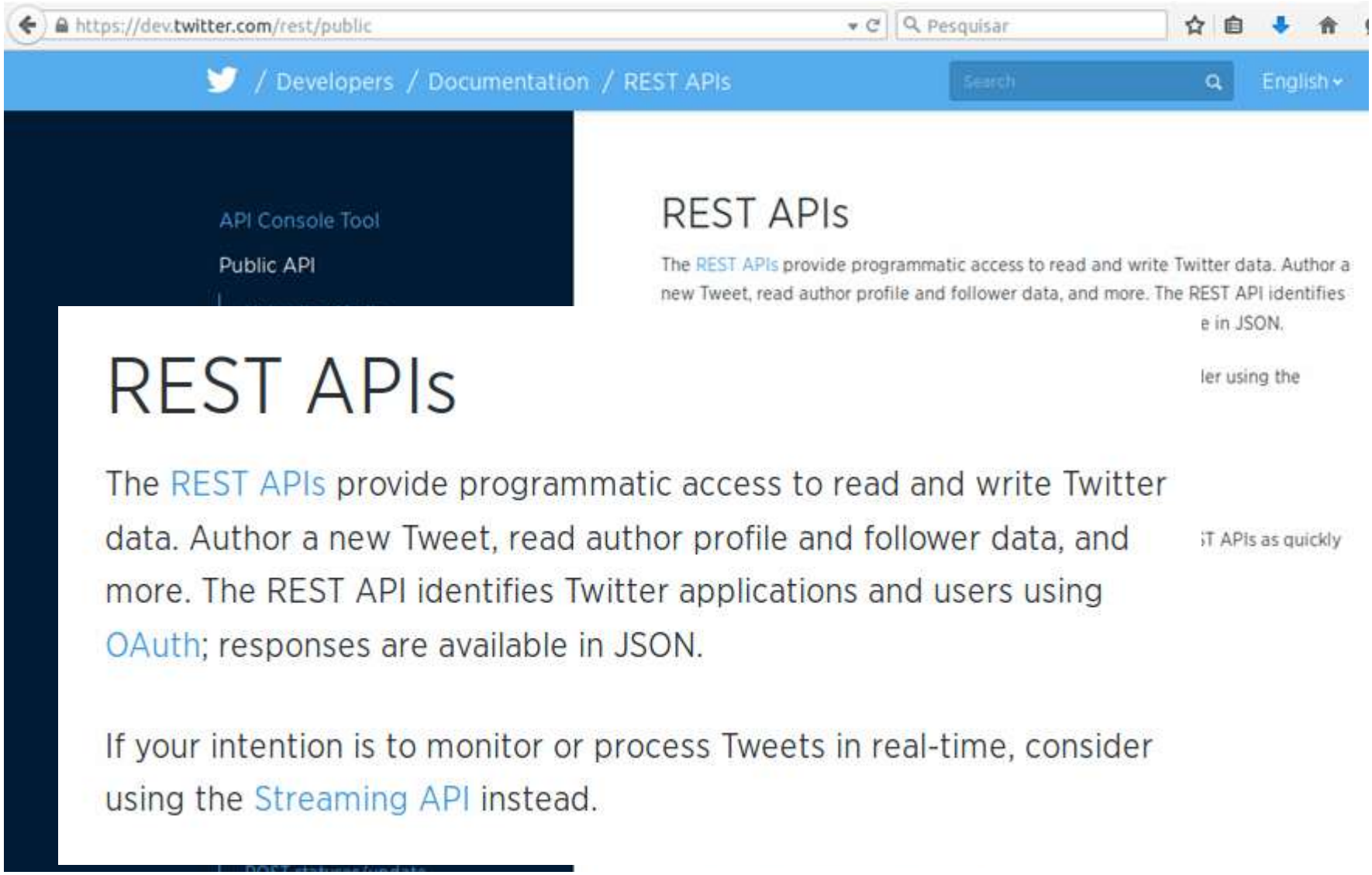


http://www.ibm.com/developerworks/br/industry/library/ind-iap-intro/

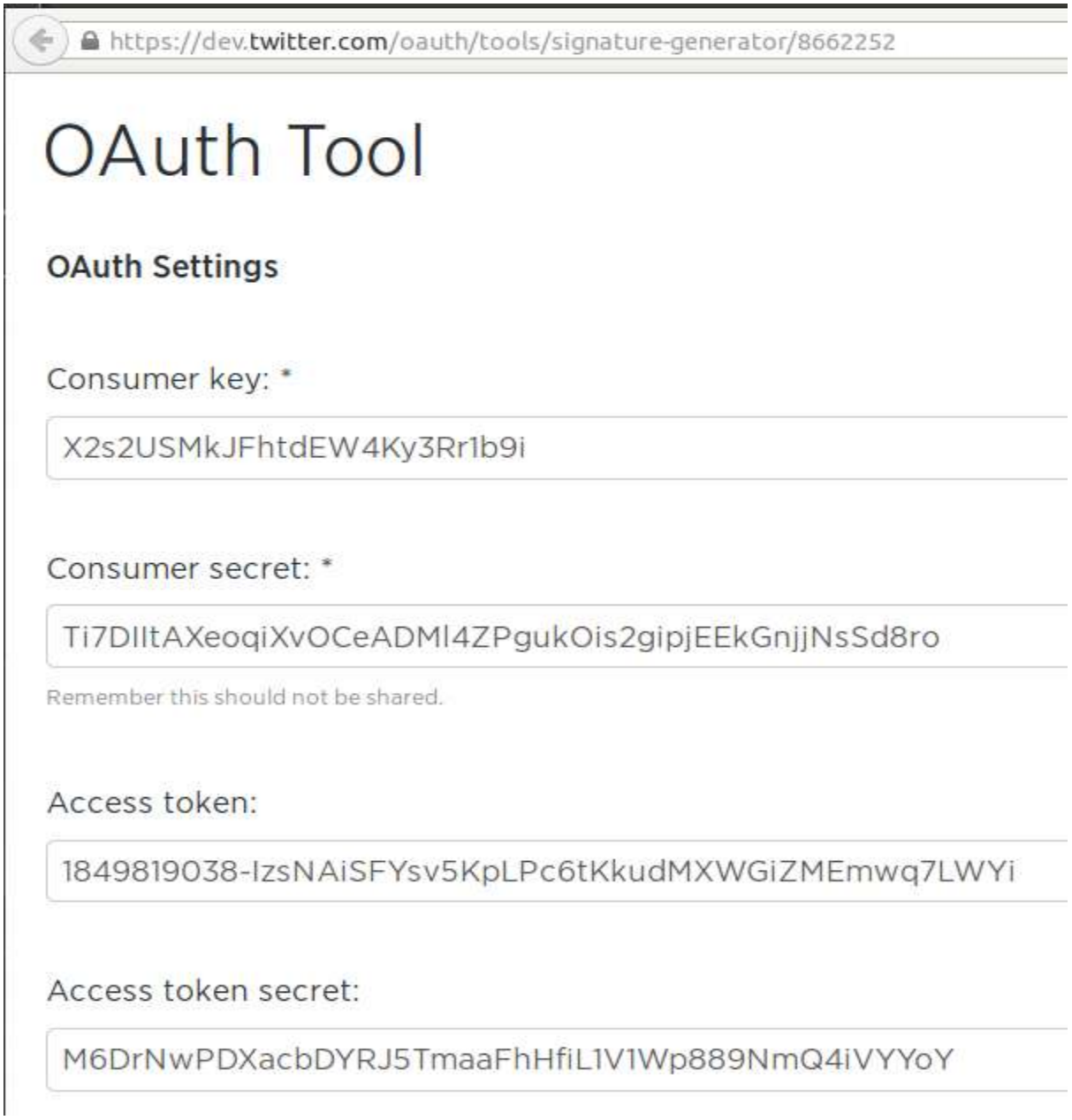
API do Twitter



API do Twitter



Acesso à API do Twitter



Scripts Python

pythoncentral.io/introduction-to-tweepy-twitter-for-python/

Python Central

Tips & Tricks | How Tos | Libraries | Tutorials | Recipes | Tools | API | About

Using tweepy

Tweepy supports accessing Twitter via Basic Authentication and the newer method, OAuth. Twitter has stopped accepting Basic Authentication so OAuth is now the only way to use the Twitter API.

Here is a sample of how to access the Twitter API using tweepy with OAuth:

```
1  import tweepy
2
3  # Consumer keys and access tokens, used for OAuth
4  consumer_key = '7EyzTcAkINVS3T2pb165'
5  consumer_secret = 'a44R7WvbMW7L8I656Y4l'
6  access_token = 'z00Xy9AkHwp8vSTJ04L0'
7  access_token_secret = 'A1cK98w2NXXaCWMqMW6p'
8
9  # OAuth process, using the keys and tokens
10 auth = tweepy.OAuthHandler(consumer_key, consumer_secret)
11 auth.set_access_token(access_token, access_token_secret)
12
   ctual interface, using authentication
```

Recebendo dados de ads.pubmatic.com...

CTIRGov

Código Python

hacked.py ×

```
#Import the necessary methods from tweepy library
from tweepy.streaming import StreamListener
from tweepy import OAuthHandler
from tweepy import Stream

#Variables that contains the user credentials to access Twitter API
consumer_key = '[redacted]i'
consumer_secret= '[redacted]'
access_token= '[redacted]'
access_token_secret= '[redacted]'

#This is a basic listener that just prints received tweets to stdout.
class StdOutListener(StreamListener):

    def on_data(self, data):
        print data
        return True

    def on_error(self, status):
        print status


if __name__ == '__main__':

    #This handles Twitter authetification and the connection to Twitter Streaming API
    l = StdOutListener()
    auth = OAuthHandler(consumer_key, consumer_secret)
    auth.set_access_token(access_token, access_token_secret)
    stream = Stream(auth, l)

    #This line filter Twitter Streams to capture data by the keywords: 'python', 'javascript', 'ruby'
    stream.filter(track=['gov.br'])
```

Chave de Busca

Mensagens

#hacked gov.br

Security Attack @Security_Attack · 13 de set
#Hacked
[redacted] Estado Mato Grosso

[redacted]mt.gov.br
zone-h.org/mirror/id/2483…

2

AnonymousOIC @AnonymousOIC · 13 de set
#Hacked[redacted]mg.gov.br HAHAHAHAHA #LaFirmaSec

1

D4RKB10 @D4RKB10 · 12 de set
#Hacked[redacted]mg.gov.br HAHAHAHAHA #LaFirmaSec @AnonMRC @Sprek3rsSec @AnonymousOIC @UnlockAnon

2

The Mentor @MentorSec · 9 de set
#HACKED

[redacted]ms.gov.br

CTIRGov

Resultado da busca

hacked.txt ×

35978895989297152,"id_str":"635978895989297152","text":"RT @juliussharpe: Now's probably
e the odds they get hacked again?","source":"\u003ca href=\"http:\/\/twitter.com\/download
003c\/a
l,"in_reply_to_status_id_str":null,"in_reply_to_user_id":null,"in_reply_to_user_id_str":null,"in_reply_to_screen_name":null,"user":
screen_name":"YoItsNino","location":"","url":null,"description":"son of samuel l
s_count":46,"friends_count":279,"listed_count":0,"favourites_count":1725,"statuses_count":650,"created_at":"Thu

":false,"lang":"en","contributors_enabled":false,"is_translator":false,"profile_background_color":"C0DEED","profile_background_image_url":"http:
93\/artprint_jimi_hendrix_big.jpg","profile_background_image_url_https":"https:\/\/

le":false,"profile_link_color":"0084B4","profile_sidebar_border_color":"C0DEED","profile_sidebar_fill_color":"DDEEF6","profile_text_color":"3333
\/YkwHuboR_normal.jpeg","profile_image_url_https":"https:\/\/pbs.twimg.com\/profile_images
banner_url":"https:\/\/pbs.twimg.com\/profile_banners\/399210320
e_image":false,"following":null,"follow_request_sent":null,"notifications":null},"geo":null,"coordinates":null,"place":null,"contributors":null,
35929454313783297,"id_str":"635929454313783297","text":"Now's probably the best time to
et hacked again?","source":"\u003ca href=\"http:\/\/www.echofon.com\/\" rel=\"nofollow

l,"in_reply_to_status_id_str":null,"in_reply_to_user_id":null,"in_reply_to_user_id_str":null,"in_reply_to_screen_name":null,"user":
rpe","screen_name":"juliussharpe","location":"Los Angeles,

rs_count":176843,"friends_count":730,"listed_count":3603,"favourites_count":24469,"statuses_count":6623,"created_at":"Wed
_zone":"Pacific Time (US &
s_enabled":false,"is_translator":false,"profile_background_color":"C0DEED","profile_background_image_url":"http:
rofile_background_image_url_https":"https:\/\/abs.twimg.com\/images\/themes\/theme1\/
_color":"0084B4","profile_sidebar_border_color":"C0DEED","profile_sidebar_fill_color":"DDEEF6","profile_text_color":"333333","profile_use_backgr
n2_normal.jpg","profile_image_url_https":"https:\/\/pbs.twimg.com\/profile_images

_profile_image":false,"following":null,"follow_request_sent":null,"notifications":null},"geo":null,"coordinates":null,"place":null,"contributors
[],"symbols":
sitive":false,"filter_level":"low","lang":"en"},"retweet_count":0,"favorite_count":0,"entities":
[{"screen_name":"juliussharpe","name":"Julius
3,16]}],"symbols":
sitive":false,"filter_level":"low","lang":"en","timestamp_ms":"1440464159377"}

35978896815484928,"id_str":"635978896815484928","text":"RT @fredthompson: IRS hacked;
ble to keep us safe, but at least they're quick with a b\u2026","source":"\u003ca href=

CTIRGov

Sumário

Agenda

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ **Estudo de caso**
- ✓ Cursos online
- ✓ Conclusões

CTIRGov

Estudo de caso

- Pesquisa acadêmica para validação uma metodologia de possível aplicação institucional.

- Coleta de dados em fontes abertas.

- Palavras norteadoras da pesquisa:
  - Ética, respeito à privacidade, observância ao ordenamento jurídico.

twitter

TANGO DOWN

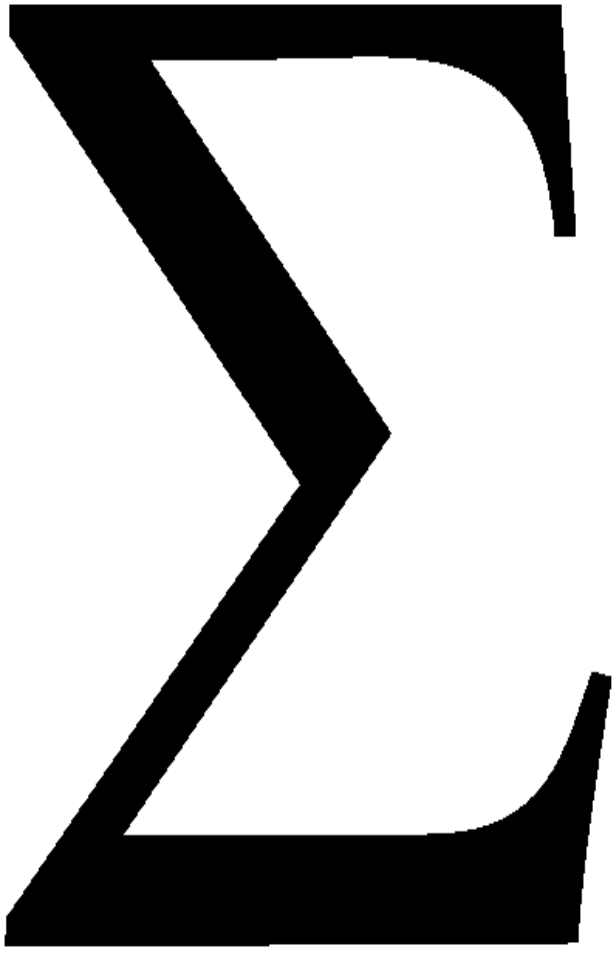
Escopo do experimento

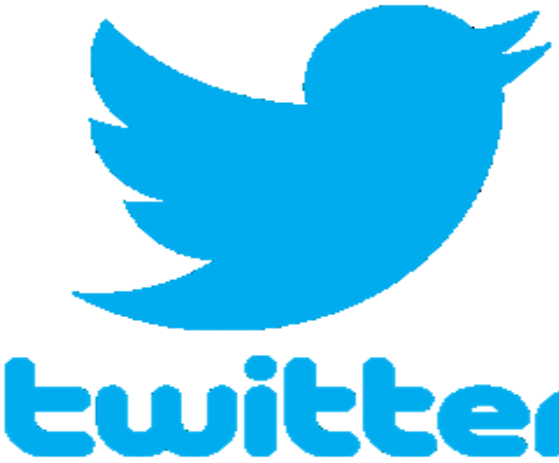
Estudo dos movimentos *hackers* denominados “operações”, contra os sítios governamentais brasileiros, e dos patrocinadores, que ocorreram antes e durante a realização da Copa do Mundo de 2014, cuja mobilização ocorreu principalmente por meio do “twitter”, pelo uso de “hashtags”.

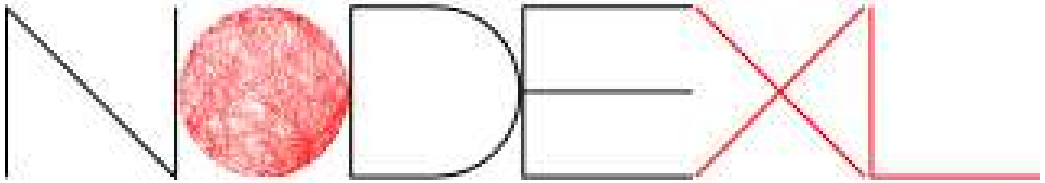
twitter

Estudo de caso

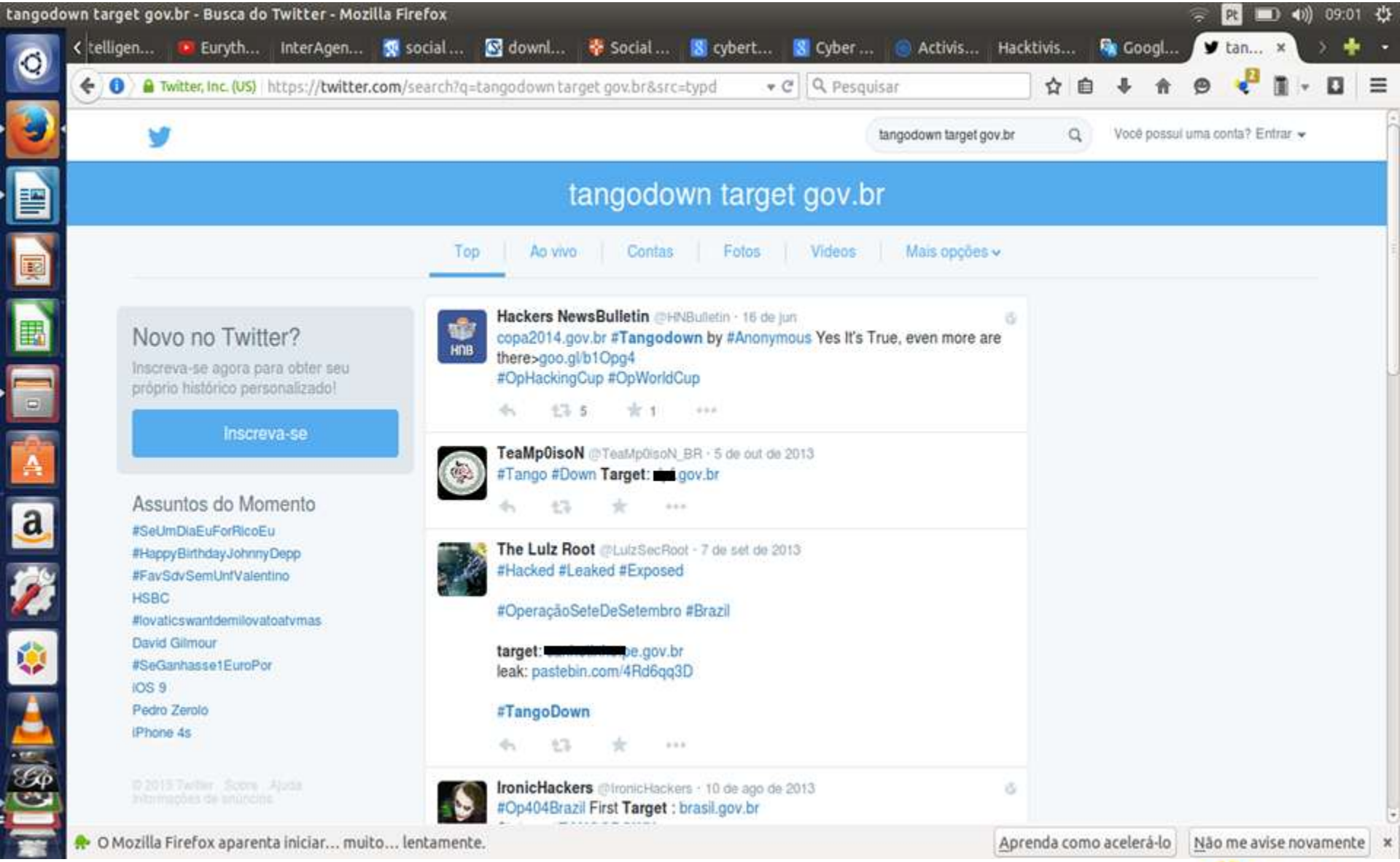
#tangodown, #OpHackingCup e #Naovaitercopa.







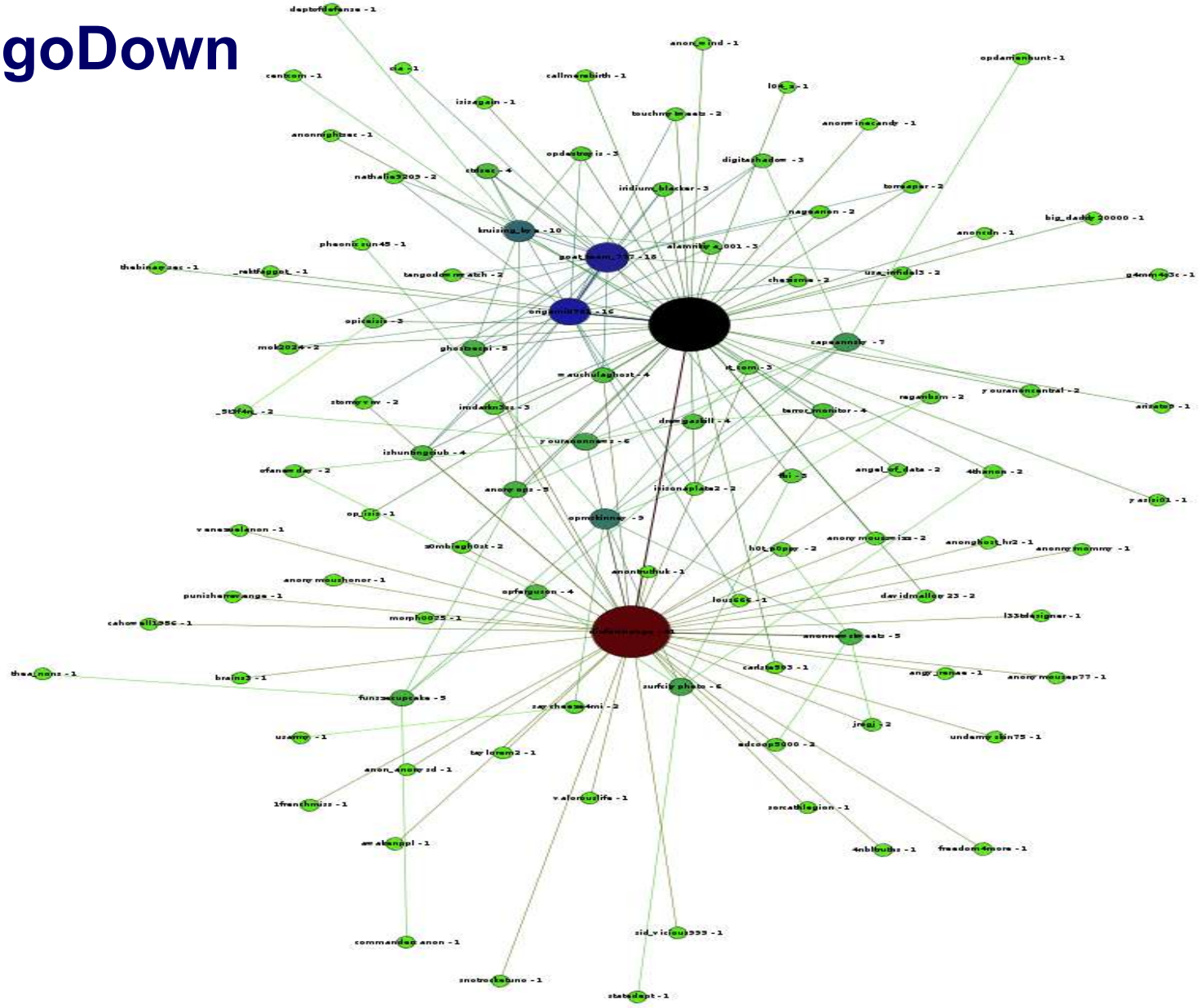
TangoDown



CTIRGov

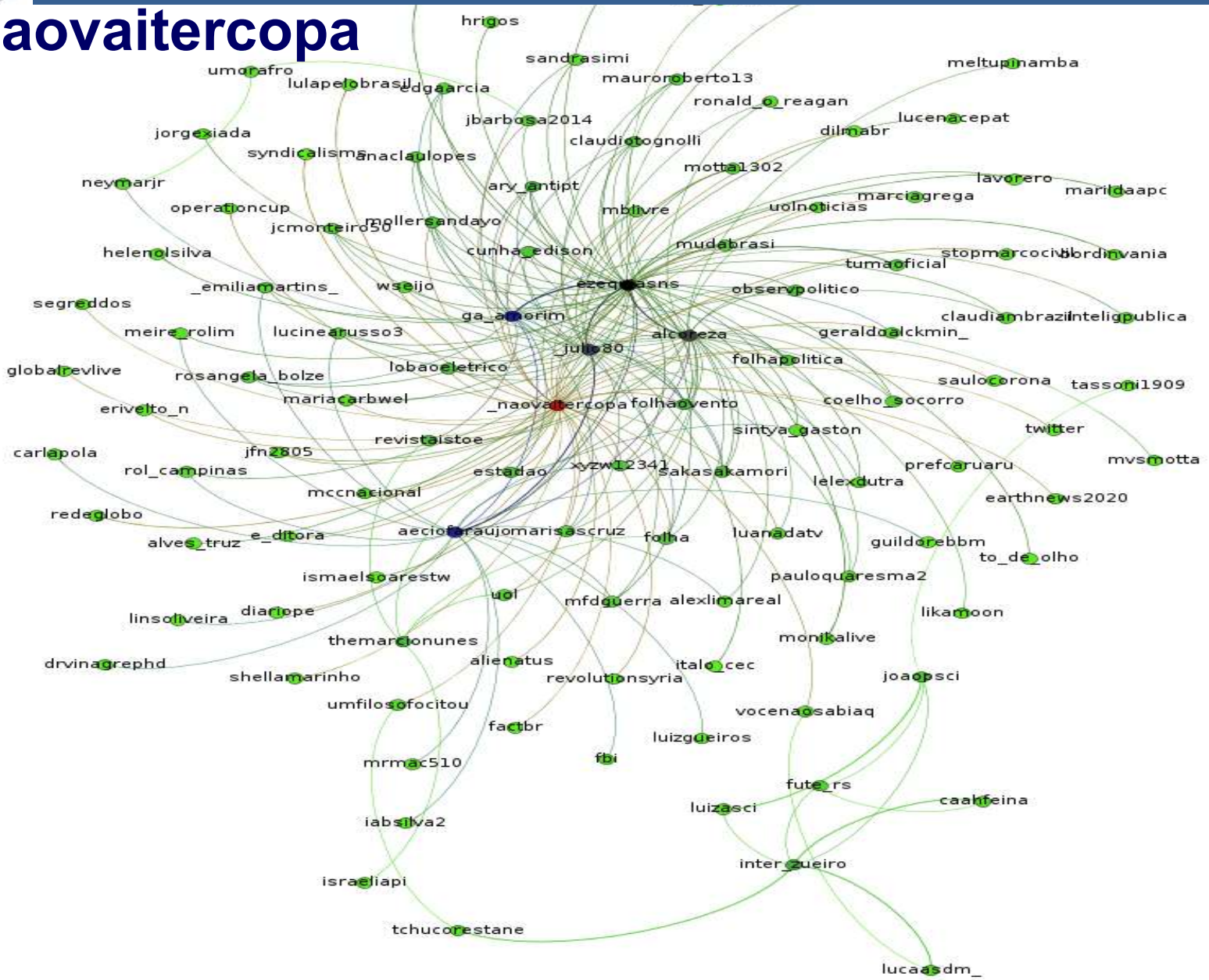
Análise dos dados

#TangoDown



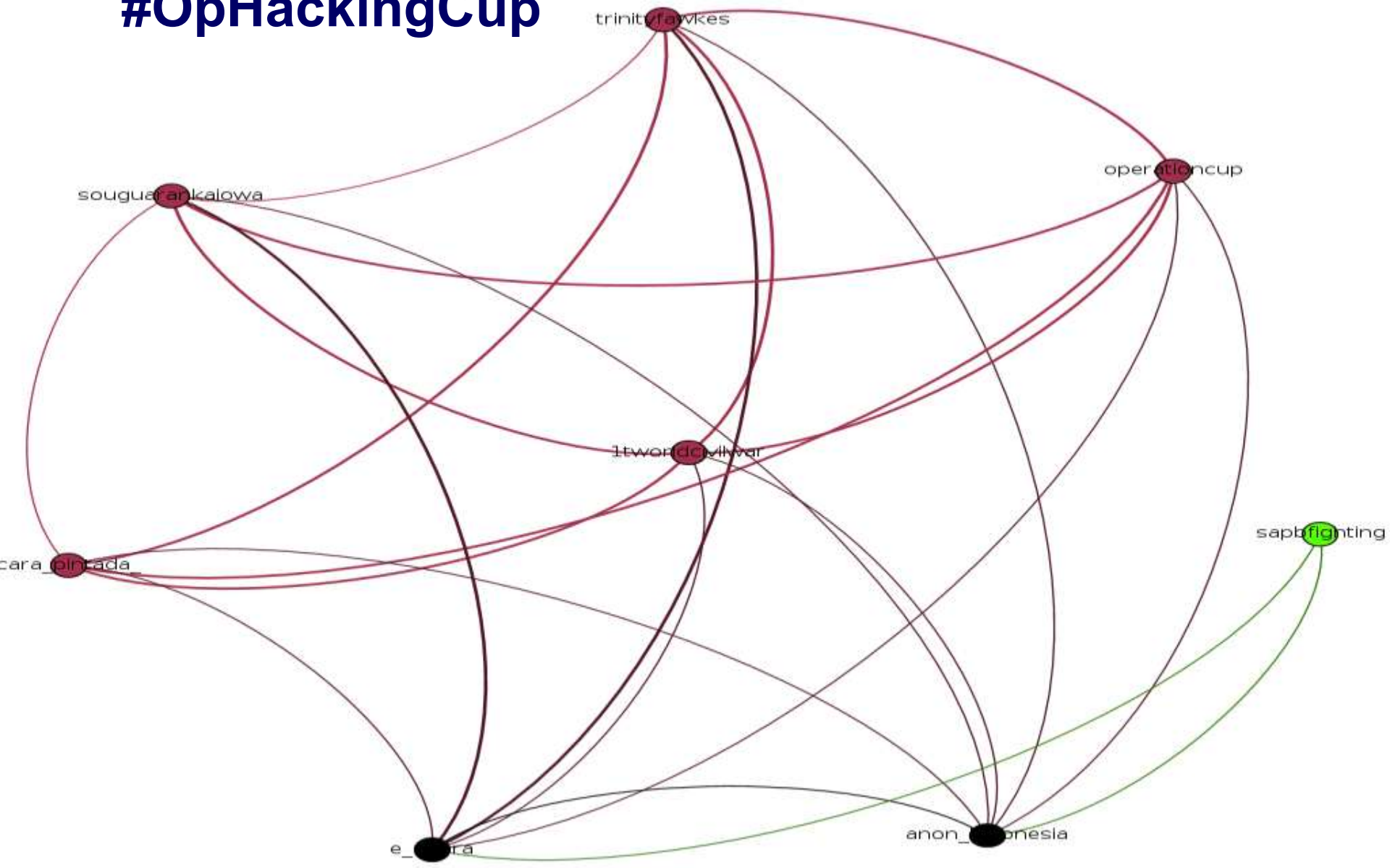
Análise dos dados

#naovaitercopa



Análise dos dados

#OpHackingCup



Principais desafios

i) Definição dos dados a serem coletados (objeto de análise);

ii) A coleta dos dados (definir as ferramentas para obtenção dos dados);

iii) visualização gráfica da rede social (análise qualitativa); e

iv) Grande volume de dados oriundo do acompanhamento contínuo das mídias sociais.

Limitações da Pesquisa

Além do desafio técnico de analisar grandes quantidades de dados, este trabalho evidenciou que a análise das informações extrapola conhecimento das áreas da computação, requerendo conhecimentos das áreas humanas, como antropologia, sociologia, psicologia, dentre outras.

Sumário

Agenda

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ **Cursos online**
- ✓ Conclusões

CTIRGov

Cursos Online

https://www.coursera.org/course/sna

UNIVERSITY OF MICHIGAN

Análise de Redes Sociais

This course will use social network analysis, both its theory and computational tools, to make sense of the social and information networks that have been fueled and rendered accessible by the internet.

coursera

Courses · alexandre Ribeiro

JOHNS HOPKINS BLOOMBERG SCHOOL of PUBLIC HEALTH

R Programming

by Roger D. Peng, PhD, Jeff Leek, PhD, Brian Caffo, PhD

Signature Track

Announcements

Course Book

WEEK-BY-WEEK

Week 1: Getting Started and R Nuts and Bolts

Week 2: Programming with R

Week 3: Loop Functions and Debugging

Week 2

Help Center

Programming with R

This week is all about functions and about controlling the flow of an R program. We start with control structures (like if-else, and for loops) and then move on to writing functions. Next, we discuss the lexical scoping features of the language and how they can be used in interesting ways, particularly for statistical applications.

Learning Objectives

By the end of this week you should be able to:

- Write an if-else expression
- Write a for loop, a while loop, and a repeat loop
- Define a function in R and specify its return value [see Functions Part 1 and Part 2]
- Describe how R binds a value to a symbol via the search list
- Define what lexical scoping is with respect to how the value of free variables are resolved in R
- Describe the difference between lexical scoping and dynamic scoping rules
- Convert a character string representing a date/time into an R datetime object. [see Dates and Times]

https://www.coursera.org/course/rprog

Cursos Online

www.leonidzhukov.net/hse/2015/networks/

Pesquisar

Structural Analysis and Visualization of Networks

Department of Data Analysis and Artificial Intelligence, School of Computer Science
National Research University Higher School of Economics

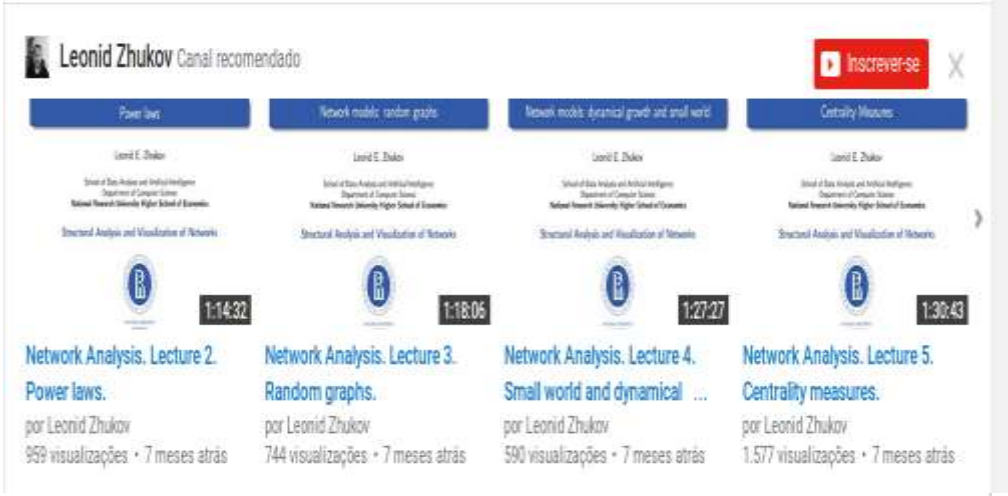
- Home
- Lectures
- Labs
- Homeworks
- Reading material
- Textbooks
- Software

Winter-Spring 2015.

Instructor: Prof. Leonid Zhukov
Teaching assistant: Andrey Shestakov

Course Outline

1. **Introduction to network science**
2. **Power laws**
3. **Models of network formation**
4. **Structure, nodes and links analysis**
5. **Network communities**
6. **Evolving networks and link prediction**
7. **Diffusion and random walks**
8. **Epidemics on networks**
9. **Diffusion of information**
10. **Influence propagation**



Module 3

Lectures

1. [15.01.2015] **Introduction to network science.** [Lecture 1] [Video]
   Introduction to the complex network theory. Network properties and metrics.
2. [20.01.2015] **Power laws.** [Lecture 2] [Video]
   Power law distribution. Scale-free networks.Pareto distribution, noramlization, moments. Zipf law. Rank-frequency plot.

CTIRGov

Sumário

Agend

- ✓ Ambientação
- ✓ Definição do tema
- ✓ A ciência de redes
- ✓ Medidas de rede
- ✓ Análise de Redes Sociais - ARS
- ✓ Grupos de Pesquisa
- ✓ Algumas ferramentas
- ✓ Estudo de caso
- ✓ Cursos online
- ✓ **Conclusões**

CTIRGov

Conclusões

O trabalho buscou avaliar uma metodologia para análise de mídias sociais no sentido de identificar grupos que promovem ações maliciosas contra as infraestruturas computacionais do Estado Brasileiro.

Trabalhos futuros

- Validação da metodologia;
- Definição da ferramentas para extração de dados;
- Aprimoramento da análise dos dados.

Referências

Barabási, A. L.; Jeong, H.; Néda, Z.; Ravasz, E.; Schubert,A. eVicsek,T. **"Evolution of the social network of scientific collaborations"**. Physica A: Statistical Mechanics and its Applications. Ed. Elsevier B.V., 2002.

Newman, M.E.J. **"The structure of scientific collaboration networks"**. PNAS – Proceedings of the National Academy of Sciences, vol. 98, Jan/2001, USA.

Paganini, P. Governments are increasing cyber security on social media. 2012. Disponível em: http://securityaffairs.co/wordpress/7827/intelligence/governments-are-increasing-cyber-security-on-social-media.html

Sampaio, R. B. "ARS Medidas – Medidas e Estruturas de Redes. Como utilizar as medidas da Rede para apoiar a determinação de suas Características Estruturais". Disponível em: https://prezi.com/wu7eebrwzz7u/ars-medidas/?utm_campaign=share&utm_medium=copy, acesso em 05/09/2015.

VOSviewer. "Software tool for constructing and visualizing bibliometric networks". Disponível em: http://www.vosviewer.com/Home,acesso em: 12/05/2015 . de 2013.

Wasserman, S; Faust,K. Social Network Analysis Methods and Applications. Cambrigde University Press, 1994.

Watts, D; Strogatz, S. Collective dynamics of small-world' networks. Artigo, Nature, Vol. 393, 1998.

Referências

http://www.barabasilab.com/resources.php

http://www.visualcomplexity.com/vc/

http://findthebacon.com/

http://www.insna.org/

http://escoladeredes.net/

https://gephi.org/

http://nodexl.codeplex.com/

http://www.casos.cs.cmu.edu/projects/ora/software.php

http://pajek.imfm.si/doku.php

http://www.yworks.com/en/products_yed_about.html

http://cran.r-project.org/

https://www.coursera.org/course/sna

http://barabasilab.neu.edu/courses/phys5116/

https://cguibourg.wordpress.com/2015/05/04/tutorial-network-analysis-of-a-twitter-hashtag-using-gephi-and-nodexl/

http://nationalsecurityzone.org/war2-0/introduction-the-science-of-networks/

http://www.casos.cs.cmu.edu/projects/ora/

http://tweettracker.fulton.asu.edu/TweetTracker_Guide.pdf

Reflexão

"O maior valor de uma fotografia é quando ela nos força a perceber coisas que nunca ' esperamos ver"

- John Tukey
- Exploratory Data Analysis (1967)

http://www.cin.ufpe.br/~rbcp/taia/2011-2/aed-redes-sociais.pptx

CTIRGov

OBRIGADO!

Alexandre Ribeiro – alejr.eb@gmail.com

http://www.ctir.gov.br

ctir@ctir.gov.br (notificação de incidentes)

cgtir@planalto.gov.br (assuntos diversos)

INOC-DBA: **10954*810**