Gone in Six Characters: Short URLs Considered Harmful for Cloud Services

Autor: Martin Georgiev e Vitaly Shmatikov

Acadêmica: Ana Cláudia Moser

URLs curtas e serviços

Encurtadores de URLs

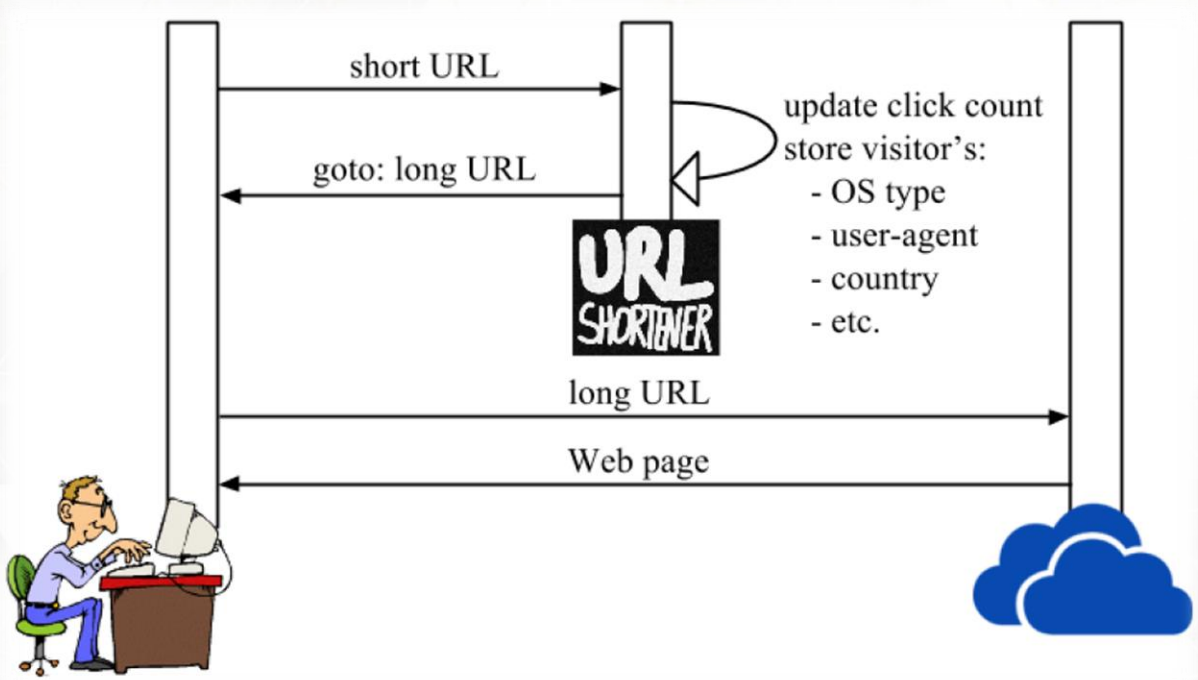
https://drive.google.com/file/d/0B6UZKSO2oqEHVXEzQ0VLSF9vWDg/view?usp=sharing

https://goo.gl/zXzmcU





Encurtadores de URL



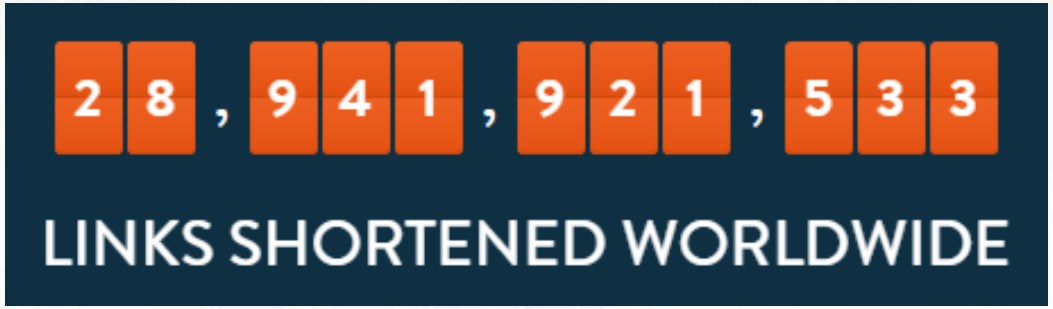
https://goo.gl/zXzmcU

Token

Key

[a-z, A-Z, 0-9] = 62^6 possibilidades

Encurtadores de URL – bit.ly

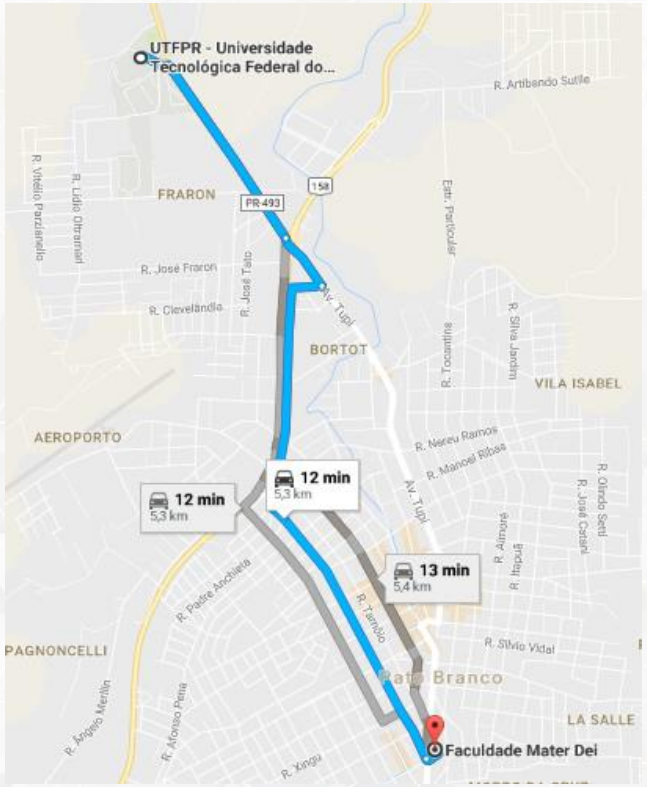


http://bit.ly/2eJ52AH

4-7 caracteres
62^6 possibilidades

ldrv.ms
binged.it
yhoo.it
mapq.st

Encurtadores de URL – goo.gl/maps



https://maps.app.goo.gl/i/7zBys

Tamanho – 5 caracteres

62^5 possibilidades

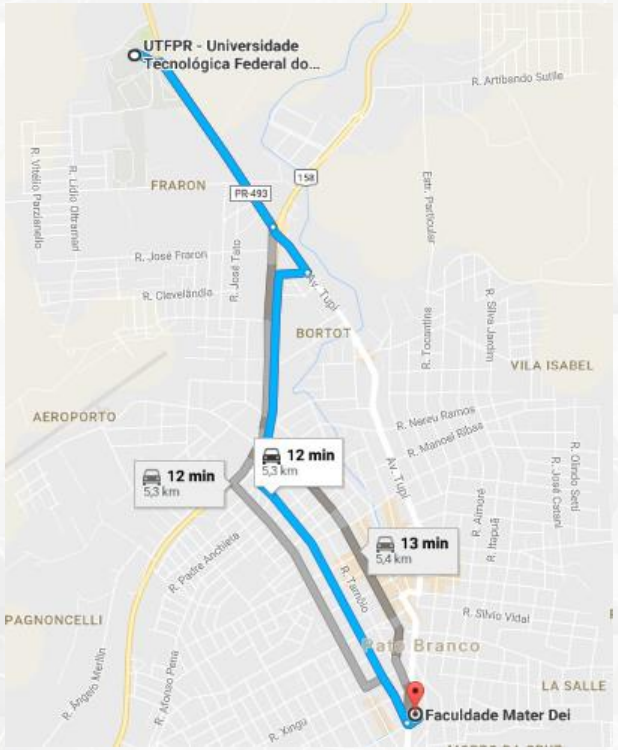
Armazenamento na nuvem

Armazenamento na nuvem

OneDrive

Permissão de visualização
Permissão de edição
Acesso público

Mapas online



https://maps.app.goo.gl/?link=https://www.google.com.br/maps/dir/UTFPR%2B-%2BUniversidade%2BTecnol%25C3%25B3gica%2BFederal%2Bdo%2BParan%25C3%25A1,%2BPato%2BBranco%2B-%2BPR/Faculdade%2BMater%2BDei%2B-%2BCentro,%2BPato%2BBranco%2B-%2BPR/@-26.2148797,-52.6979971,14z/data%3D!3m1!4b1!4m13!4m12!1m5!1m1!1s0x94e5534653e77ca5:0x23ed25fac7459476!2m2!1d-52.6895744!2d-26.1956431!1m5!1m1!1s0x94e55292b5aa4fe3:0x165da9324c9160ec!2m2!1d-52.6715492!2d-26.2337283?utm_source%3Dapp-invite%26mt%3D8%26pt%3D9008%26utm_medium%3DSIMPLE%26utm_campaign%3Ds2e-ai%26ct%3Ds2e-ai&apn=com.google.android.apps.maps&amv=703000000&isi=585027354&ibi=com.google.Maps&ius=comgooglemapsurl&utm_source=app-invite&mt=8&pt=9008&utm_medium=SIMPLE&utm_campaign=s2e-ai&ct=s2e-ai&invitation_id=493454522602-4652e5e2-00d8-47b7-a1cb-d4c225def64c

https://maps.app.goo.gl/i/7zBys

Escaneando URLs curtas

Razão de escaneamento

- bit.ly
  - O acesso a API é limitado à 5 conexões simultâneas para um cliente.
  - 2.6 queries/seconds
- goo.gl/maps
  - 1.000.000 queries/day

Escaneando URLs curtas

Amostragem

- Alfabeto: [a-z, A-Z ,0-9]
- Geração de *tokens* únicos para cada serviço dentro do espaço de *tokens*

Escaneando URLs curtas

- bit.ly
  - 100.000.000 de *tokens* de 6 caracteres.
  - Acessando a base de dados através de 189 máquinas
  - Encontradas: 42.229.055 URLs mapeadas.
  - 7 caracteres – 29.331.088 URLs mapeadas
- goo.gl/maps
  - Gerados 63.970.000 *tokens*
  - 23.965.718 URLs mapeadas

Escaneando URLs curtas

Enumeração exaustiva

- Enumeração total do bit.ly
  - 12.2 milhões de horas
  - 510.000 *client-days*
  - $36.700 usando instâncias dos computadores da Amazon
- Enumeração total do goo.gl – antes das mudanças
  - 916 *client-days*

URLs curtas e Serviços de armazenamento em nuvem

- 42.229.055 do bit.ly (6 caracteres)
  - 3.003 OneDrive: 2130 de contas distintas e 150 com permissão de edição em arquivo
  - 16.521 SkyDrive
  - 245.000 *client-days* para mapear todas as pastas do OneDrive e SkyDrive
- 29.331.099 do bit.ly (7 caracteres)
  - 25.594 OneDrive
  - 21.487 SkyDrive

Formato de link do Onedrive

File type	prefix	path	cid	id	resid	app	v	ithint	authkey
Word	https://onedrive.live.com	/view*	✓	✗	✓	✓	✗	✗	optional
Excel		/view or /edit	✓	✗	✓	✓	✗	✗	
PowerPoint		/view*	✓	✗	✓	✓	✗	✗	
OneNote		/view or /edit	✓	✗	✓	✓	✗	✗	
PDF		/view	✓	✗	✓	✓	✗	✗	
Surveys		/survey	✗	✗	✓	✗	✗	✗	
Media files		/	✓	✓	✗	✗	✓	✗	
Downloads		/download.aspx	✓	✗	✓	✗	✗	✗	
Folders		/ +	✓	✓	✗	✗	✗	✓	

Formato de link do Onedrive

http://1drv.ms/1xNOWV7

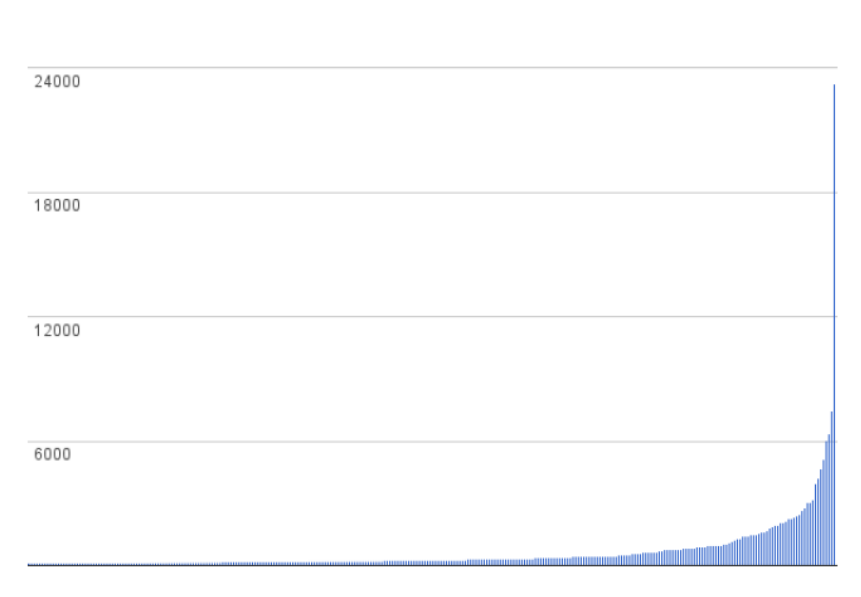
https://onedrive.live.com/?**cid**=485bef1a80539148&**id**=485BEF1A80539148!115&**ithint**=folder,xlsx&**authkey**=!AOOp2TqTTSMT5

URL para raiz da conta: https://onedrive.live.com/?cid=**XXX**&authkey=**YYY**

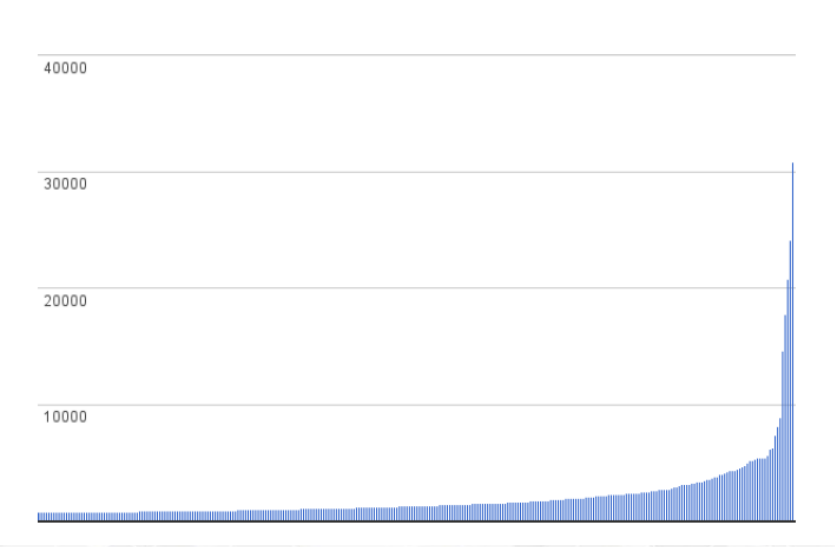
Contas OneDrive

File type	# of files found in 6-char sample space	# of files found in 7-char sample space
Word	2,116	21,077
Excel	921	6,050
PowerPoint	688	5,068
OneNote	51	6
PDF	10,080	41,465
Surveys	22	226
Media files	204,735	862,641
Downloads*	8,663	168,613

Distribuição de arquivos por conta



Token 6 caracteres

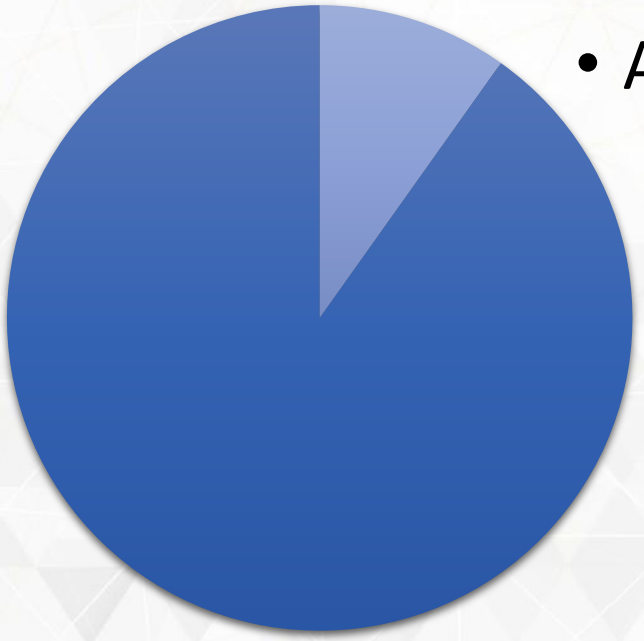


Token 7 caracteres

GoogleDrive

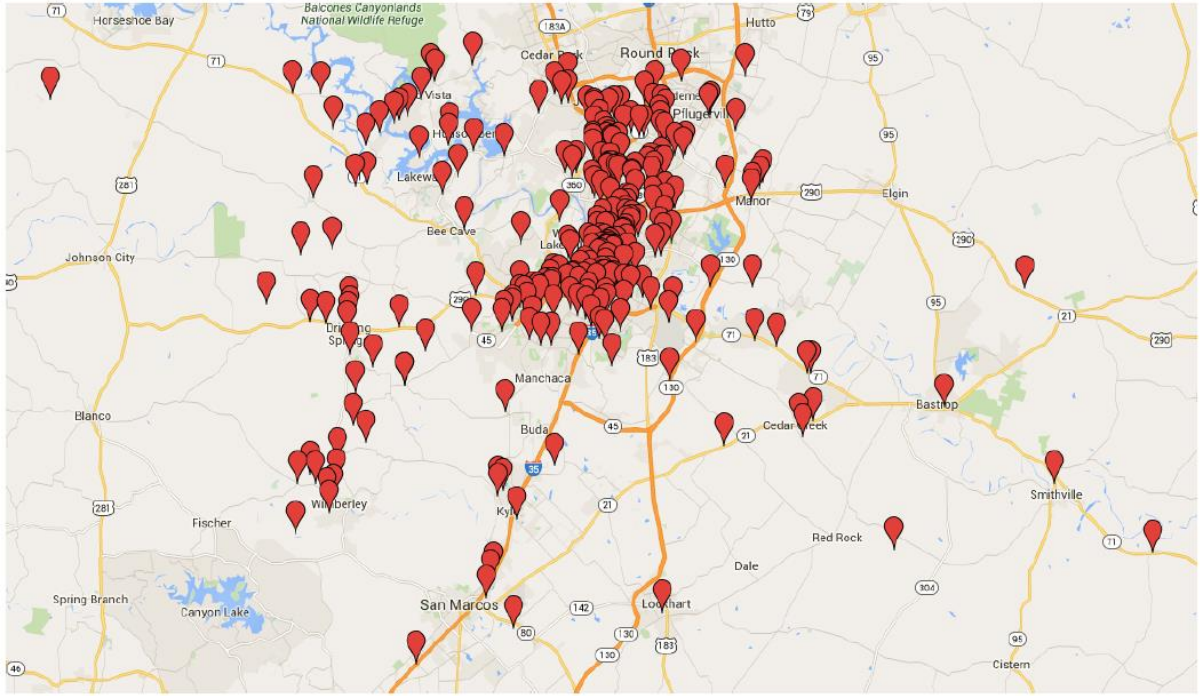
- Scan com 6 caracteres em bit.ly levou a 44 links para pastas
  - 30 com permissão de visualização
  - 3 com permissão de escrita
  - 7 desativados
  - 4 com proteção de permissão
- Scan com 7 caracteres em bit.ly levou a 414 links para pastas
  - 277 com permissão de visualização
  - 40 com permissão de escrita
  - 49 desativados
  - 48 com proteção de permissão

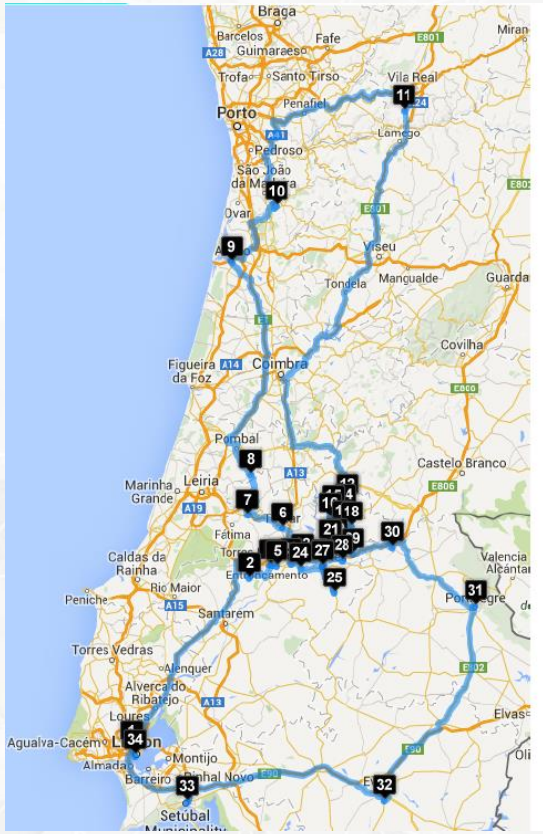
URLs curtas em mapas online



- Amostra total: 23.965.718
  - 3.913 direções começando em um hospital e terminando em uma residência
  - 12.668 direções começando em uma residência e terminando em um hospital

URLs curtas em mapas online





Sugestões

- Fazer URLs curtas, mais longas
- Informar os usuários sobre os riscos
- Não confiar em encurtadores de URL universal
- Adicionar CAPTHAs ou outros métodos
- Fazer APIs melhores

Gone in Six Characters: Short URLs Considered Harmful for Cloud Services

Autor: Martin Georgiev e Vitaly Shmatikov

Acadêmica: Ana Cláudia Moser