TROOPERS
MAKE THE WORLD A SAFER PLACE

The Social Map

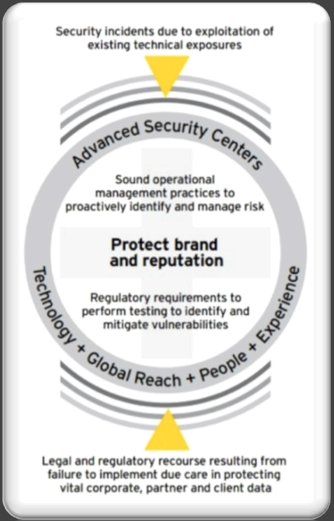
Johnny Deutsch
Hacktics Advanced security Center

ERNST & YOUNG
Quality In Everything We Do

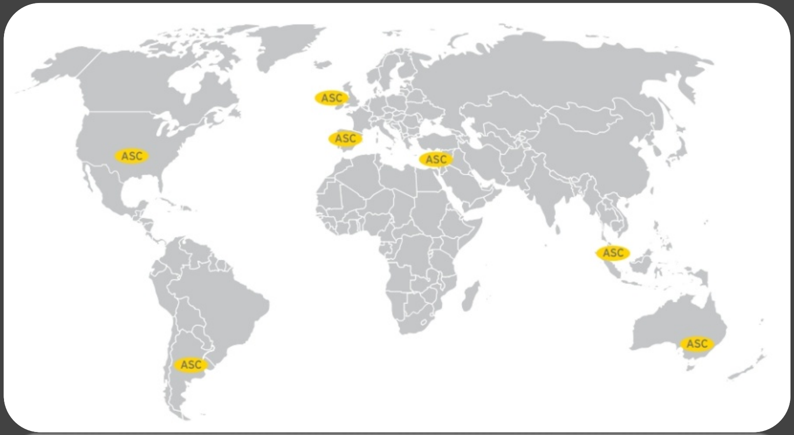
Who are you ?

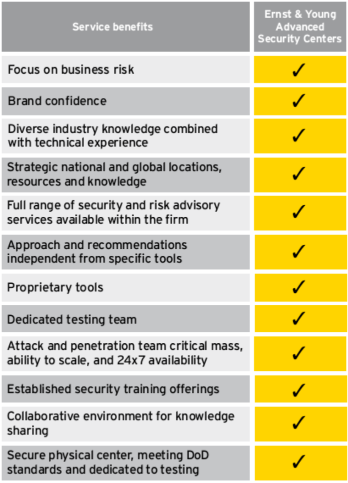
- Ex Army Officer
- Consultant for the MoD
- Heads up HASC’s Cyber Research Practice
- A Scotch lover (Laphroaig…)

EY Advanced Security Center


Security incidents due to exploitation of existing technical exposures
Advanced Security Centers
Sound operational management practices to proactively identify and manage risk
Protect brand and reputation
Regulatory requirements to perform testing to identify and mitigate vulnerabilities
Technology + Global Reach + People + Experience
Legal and regulatory recourse resulting from failure to implement due care in protecting vital corporate, partner and client data

Our Global ASC Locations:





Service benefits	Ernst & Young Advanced Security Centers
Focus on business risk	✓
Brand confidence	✓
Diverse industry knowledge combined with technical experience	✓
Strategic national and global locations, resources and knowledge	✓
Full range of security and risk advisory services available within the firm	✓
Approach and recommendations independent from specific tools	✓
Proprietary tools	✓
Dedicated testing team	✓
Attack and penetration team critical mass, ability to scale, and 24x7 availability	✓
Established security training offerings	✓
Collaborative environment for knowledge sharing	✓
Secure physical center, meeting DoD standards and dedicated to testing	✓

Our Advanced Security Research Team:

HACKTICS

- Former Military Intelligence outfit.
- Acquired by Ernst & Young (Jan 2011).
- Currently the largest IT security center in Israel – over 35 consultants.

Selected vulnerabilities published within the last two years

- Adobe: ColdFusion (CVE-2011-2463, CVE-2011-4368).
- IBM: WebSphere (CVE-2010-0714).
- Microsoft: SharePoint (CVE-2010-0716).

Planned:

- Polycom: DoS.
- InsightX: NAC Bypass.
- Oracle: eBusiness.

Here we go !

- So, let’s be social :
  - The side effect of information security – Marketing.
  - Facebook and You !

Marketing - The side effect of info-sec that we don't talk about

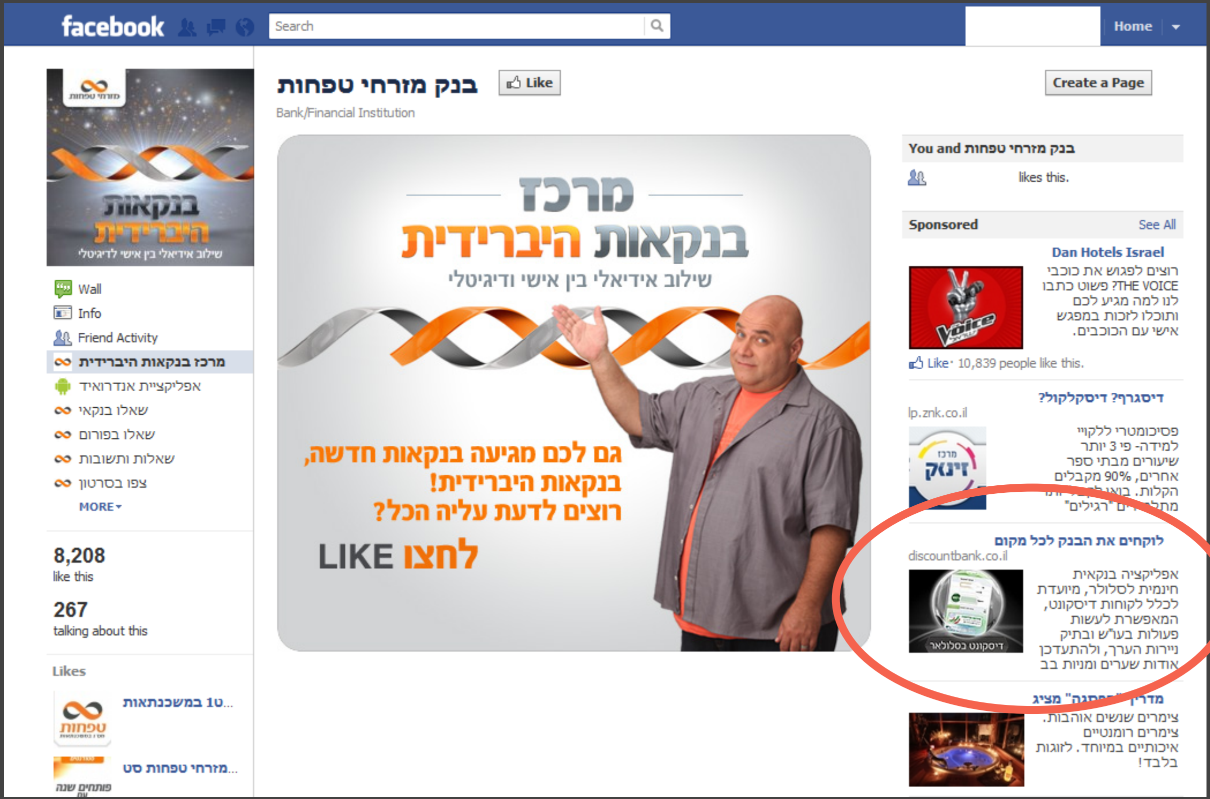
WORST PRODUCT NAME EVER
Proof that there are no women involved in the big decisions at Apple.

Marketing - The side effect of info-sec that we don’t talk about

- Isn’t this what the marketing department is all about ?
  - In an ideal world – yep.
- And again, why us ?
  - Hardening you server, is clearly Info-Sec – right ?
  - But what about hardening your brand’s Facebook page ?

What harm can come my way ?

- ▶ Did you ever see a commercial of your competing bank inside the bank ?



בנק מזרחי טפחות Like

Bank/Financial Institution

Create a Page

- Wall
- Info
- Friend Activity
- מרכז בנקאות היברידית
- אפליקציית אנדרואיד
- שאלו בנקאי
- שאלו בפורום
- שאלות ותשובות
- צפו בסרטון
- MORE

8,208
like this

267
talking about this

Likes

טו במשכנתאות1...

מזרחי טפחות סט...

You and בנק מזרחי טפחות

likes this.

Sponsored See All

Dan Hotels Israel

רוצים לפגוש את כוכבי
THE VOICE? פשוט כתבו
לנו למה מגיע לכם
ותוכלו לזכות במפגש
אישי עם הכוכבים.

Like · 10,839 people like this.

דיסגרף? דיסקלקולי?

lp.znk.co.il

פסיכומטרי ללקויי
למידה- פי 3 יותר
שיעורים מבתי ספר
אחרים, 90% מקבלים
הקלות. בואו ל[illegible]
מתל[illegible]ים "רגילים"

לוקחים את הבנק לכל מקום

discountbank.co.il

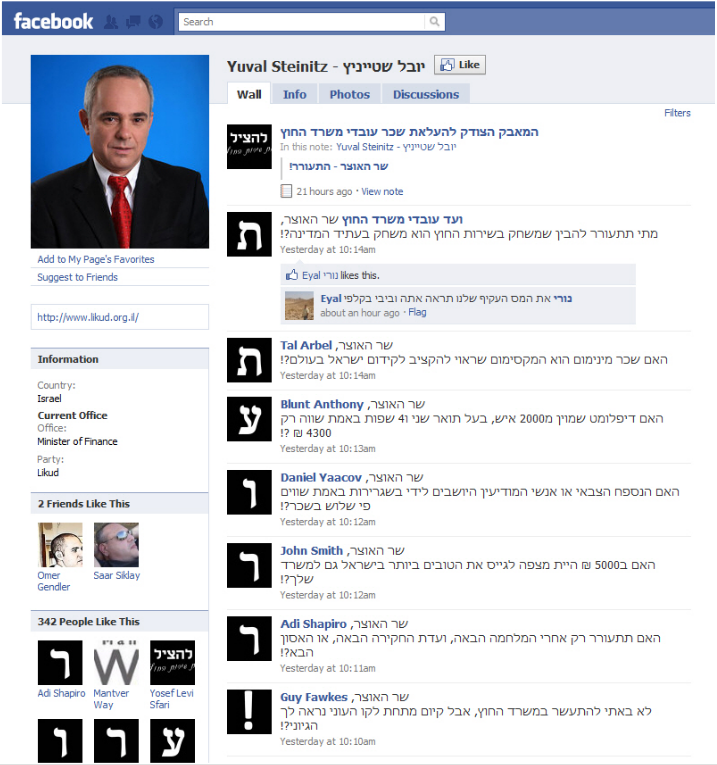
אפליקציה בנקאית
חינמית לסלולר, מיועדת
לכלל לקוחות דיסקונט,
המאפשרת לעשות
פעולות בעו"ש ובתיק
ניירות הערך, ולהתעדכן
אודות שערים ומניות בב

מדריך "[illegible]" מציג

צימרים שנשים אוהבות.
צימרים רומנטיים
איכותיים במיוחד. לזוגות
בלבד!

So your not that popular …

- ► Controlling IT.



facebook Search

Yuval Steinitz - יובל שטייניץ Like

Wall Info Photos Discussions

Filters

המאבק הצודק להעלאת שכר עובדי משרד החוץ
In this note: Yuval Steinitz - יובל שטייניץ
שר האוצר - התעורר!
21 hours ago · View note

ועד עובדי משרד החוץ שר האוצר,
מתי תתעורר להבין שמשחק בשירות החוץ הוא משחק בעתיד המדינה?!
Yesterday at 10:14am
Eyal נורי likes this.
Eyal נורי את המס העקיף שלנו תראה אתה וביבי בקלפי
about an hour ago · Flag

Tal Arbel שר האוצר,
האם שכר מינימום הוא המקסימום שראוי להקציב לקידום ישראל בעולם?!
Yesterday at 10:14am

Blunt Anthony שר האוצר,
האם דיפלומט שמוין מ2000 איש, בעל תואר שני ו4 שפות באמת שווה רק
4300 ₪ ?!
Yesterday at 10:13am

Daniel Yaacov שר האוצר,
האם הנספח הצבאי או אנשי המודיעין היושבים לידי בשגרירות באמת שווים
פי שלוש בשכר?!
Yesterday at 10:12am

John Smith שר האוצר,
האם ב5000 ₪ היית מצפה לגייס את הטובים ביותר בישראל גם למשרד
שלך?!
Yesterday at 10:12am

Adi Shapiro שר האוצר,
האם תתעורר רק אחרי המלחמה הבאה, ועדת החקירה הבאה, או האסון
הבא?!
Yesterday at 10:11am

Guy Fawkes שר האוצר,
לא באתי להתעשר במשרד החוץ, אבל קיום מתחת לקו העוני נראה לך
הגיוני?!
Yesterday at 10:10am

Add to My Page's Favorites
Suggest to Friends

http://www.likud.org.il/

Information
Country:
Israel
Current Office
Office:
Minister of Finance
Party:
Likud

2 Friends Like This
Omer Gendler
Saar Siklay

342 People Like This
Adi Shapiro
Mantver Way
Yosef Levi Sfari

facebook

Friends אגד

Wall Info Photos Notes

Enough with marketing. Moving on…

Facebook and you

- What organizations need to know about it.
- It can hurt the individual as well … but you know

Let's put things into context

- There is a lot of hype on APT's.
- You always hear of "advance intelligence gathering methods", Why ?
  - Technical information (infrastructure, client side applications…).
  - Who's he attacking.

  - The "why" is not relevant any more – it's money

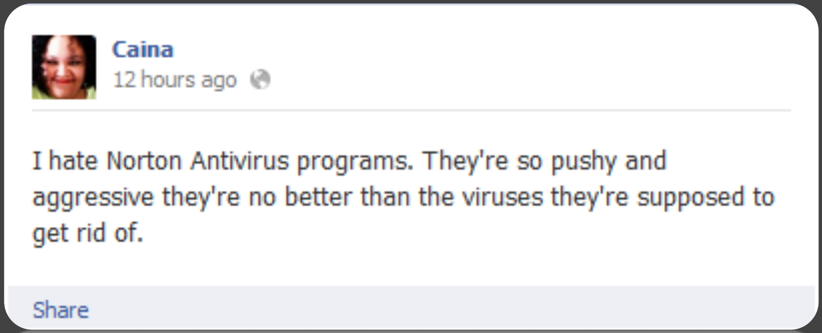
Organizations tend to think that there is only one issue with social networks:

WEAPONS OF
f
t
You
Tube
MASS DISTRACTION

There’s no patch for human stupidity !

Client side disclosure

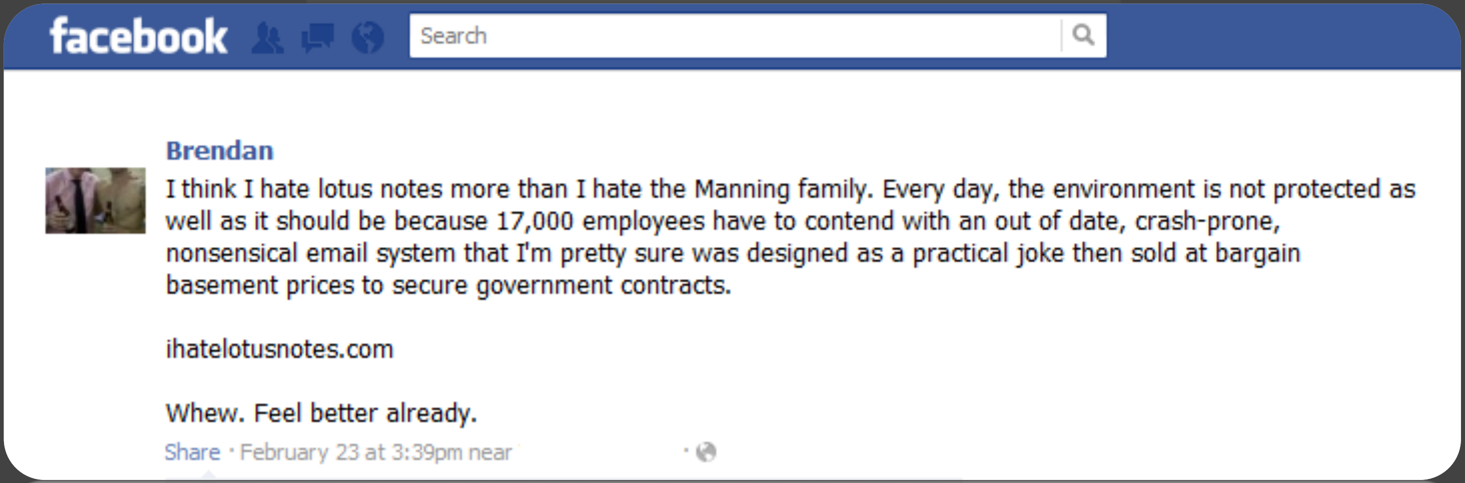
- ► Sticks and bones may break my bones, but words …



Caina
12 hours ago

I hate Norton Antivirus programs. They're so pushy and aggressive they're no better than the viruses they're supposed to get rid of.

Share



Brendan
I think I hate lotus notes more than I hate the Manning family. Every day, the environment is not protected as well as it should be because 17,000 employees have to contend with an out of date, crash-prone, nonsensical email system that I'm pretty sure was designed as a practical joke then sold at bargain basement prices to secure government contracts.

ihatelotusnotes.com

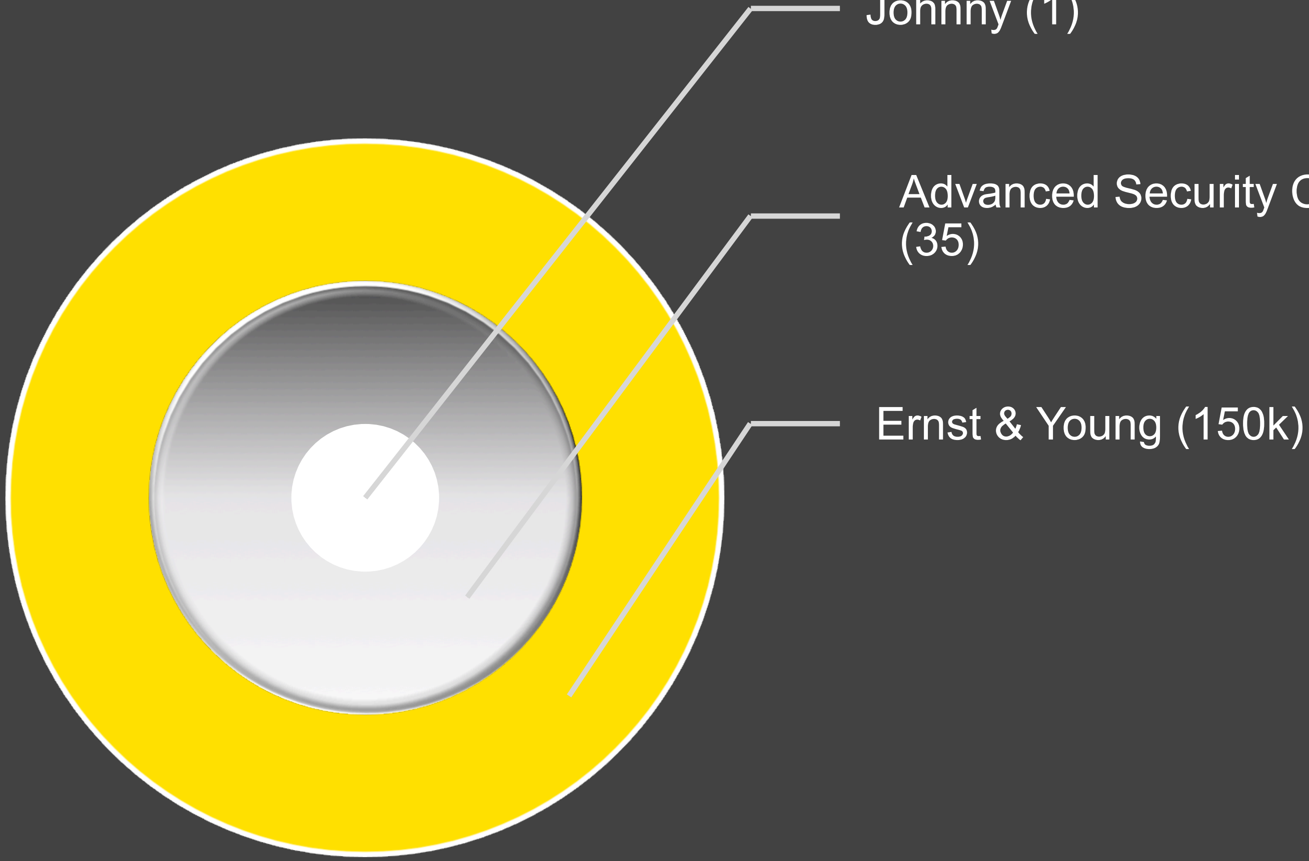
Whew. Feel better already.

Share · February 23 at 3:39pm near

Mapping you

- Multiple ways of attacking your target…
- But an art of itself is knowing how to aim your spear !

What’s the problem ?



Johnny (1)

Advanced Security Center (35)

Ernst & Young (150k)

Simulate a real world attacker

- Has some but not all of the needed info
  - He knows Johnny
  - He knows that he works at Ernst & Young
- What’s available to him ?

Maybe do no evil ?

- Google hacking ?
  - site:facebook.com "Works at" + "Ernst & Young" + "yonni“
  - Small indexing war prevents this…

Maybe the Harvester ?

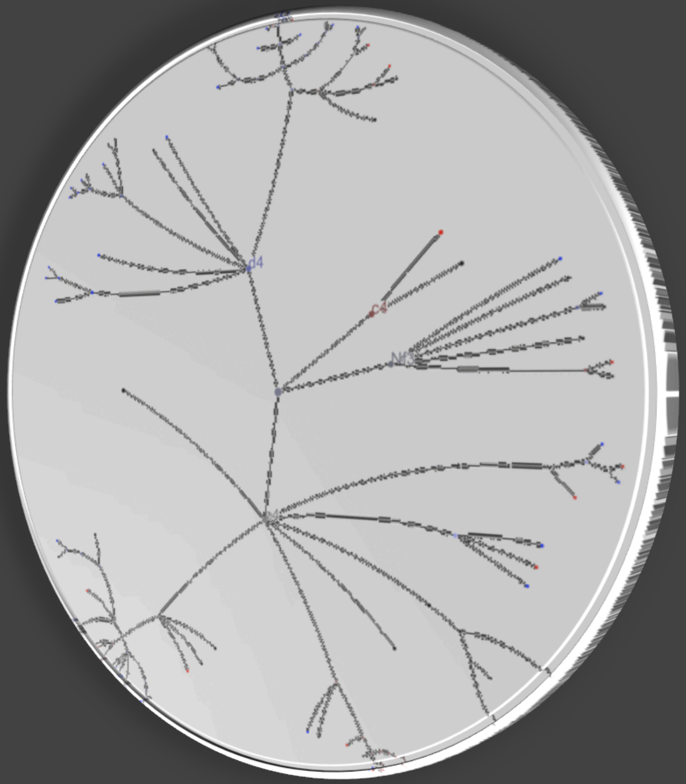
- Google - emails,subdomains/hostnames
- Google profiles - Employee names
- Bing search - emails, subdomains/hostnames,virtual hosts
- Pgp servers - emails, subdomains/hostnames
- Linkedin - Employee names
- Exalead - emails,subdomain/hostnames

But it doesn't really help us here ….

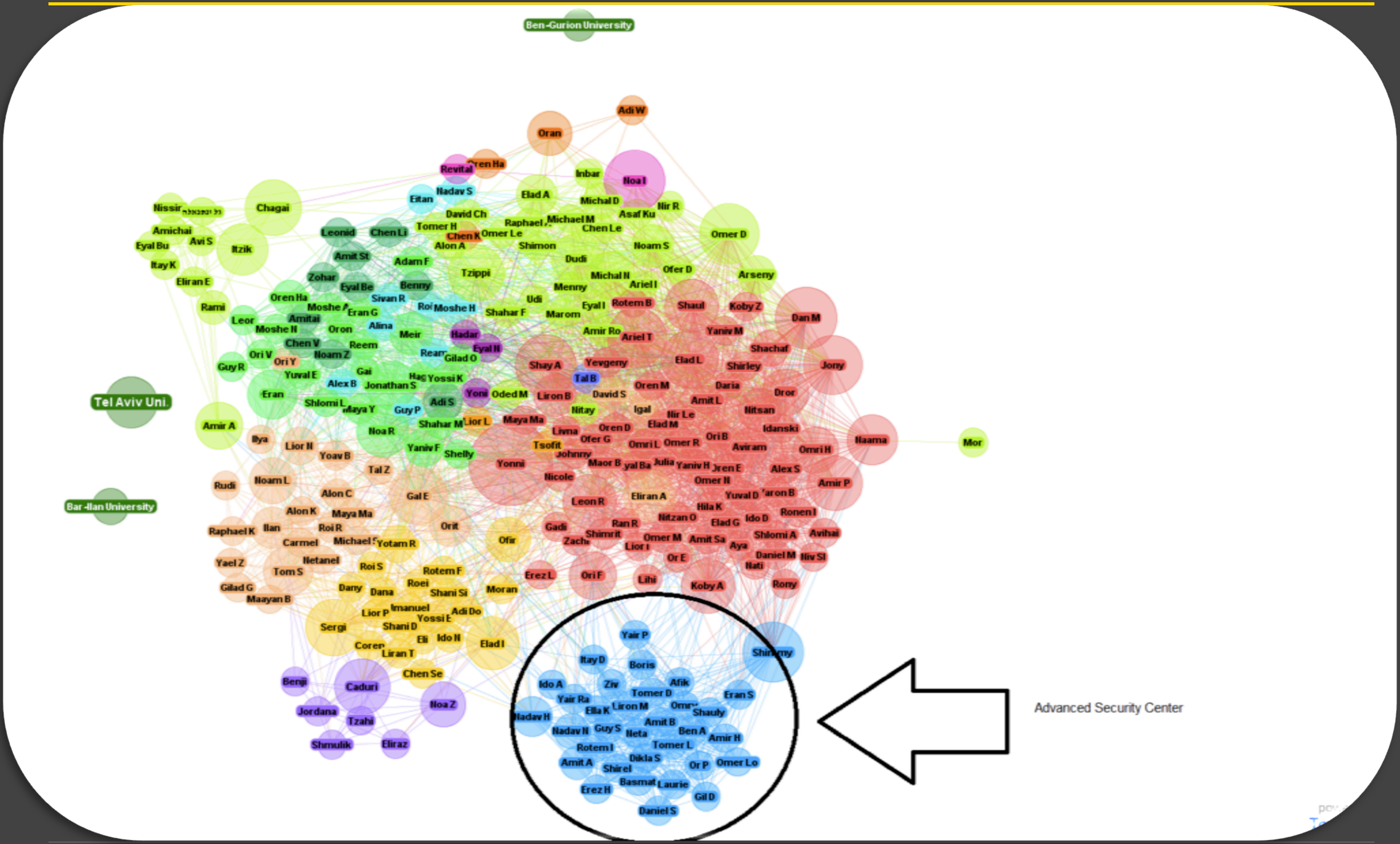
Ever heard of TouchGraph ?

TouchGraph

- ► Basically a Hyperbolic tree of your Facebook account.



And it looks like this :

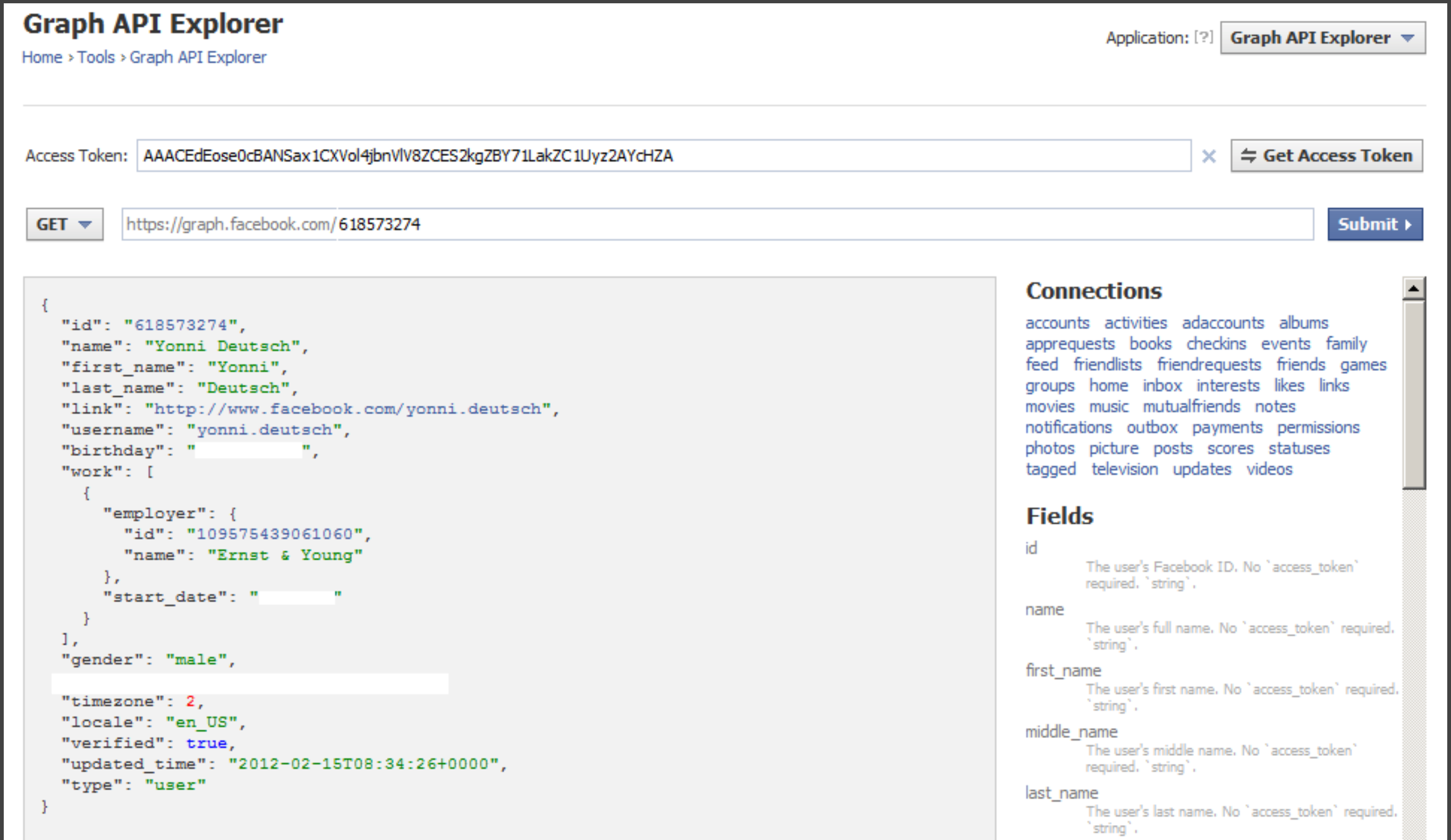


Found it !

- Not really, That’s cheating …
- Cuz it’s my own profile ….

How does TouchGraph do it ?

- API



Graph API Explorer

Home › Tools › Graph API Explorer
Application: [?] Graph API Explorer

Access Token: AAACEdEose0cBANSax1CXVol4jbnVlV8ZCES2kgZBY71LakZC1Uyz2AYcHZA

GET https://graph.facebook.com/618573274

```
{
  "id": "618573274",
  "name": "Yonni Deutsch",
  "first_name": "Yonni",
  "last_name": "Deutsch",
  "link": "http://www.facebook.com/yonni.deutsch",
  "username": "yonni.deutsch",
  "birthday": "[redacted]",
  "work": [
    {
      "employer": {
        "id": "109575439061060",
        "name": "Ernst & Young"
      },
      "start_date": "[redacted]"
    }
  ],
  "gender": "male",
[redacted]
  "timezone": 2,
  "locale": "en_US",
  "verified": true,
  "updated_time": "2012-02-15T08:34:26+0000",
  "type": "user"
}
```

Connections

accounts activities adaccounts albums apprequests books checkins events family feed friendlists friendrequests friends games groups home inbox interests likes links movies music mutualfriends notes notifications outbox payments permissions photos picture posts scores statuses tagged television updates videos

Fields

id
The user's Facebook ID. No `access_token` required. `string`.

name
The user's full name. No `access_token` required. `string`.

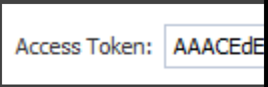
first_name
The user's first name. No `access_token` required. `string`.

middle_name
The user's middle name. No `access_token` required. `string`.

last_name
The user's last name. No `access_token` required. `string`.

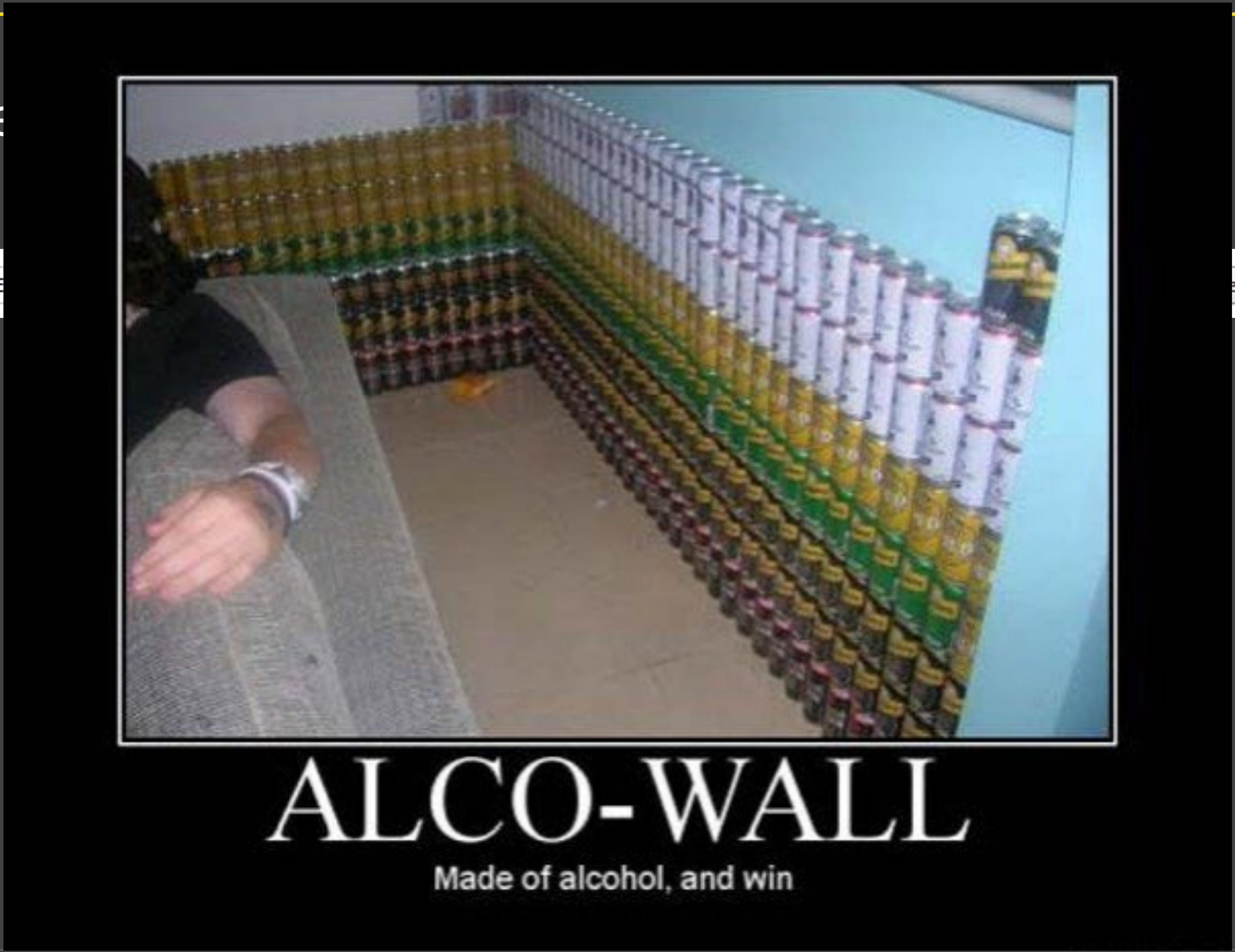
So what's the issue here?

- The



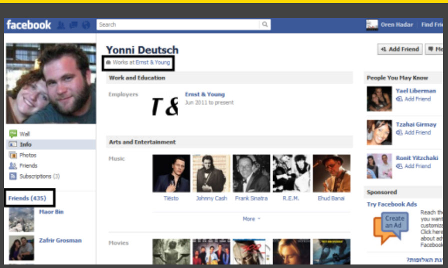
Access Token: AAACEdE

et Access Token



So how do we get it ?

- ▶ There's my profile page.



Yonni Deutsch

Works at Ernst & Young

Work and Education

Employers: Ernst & Young, Jun 2011 to present

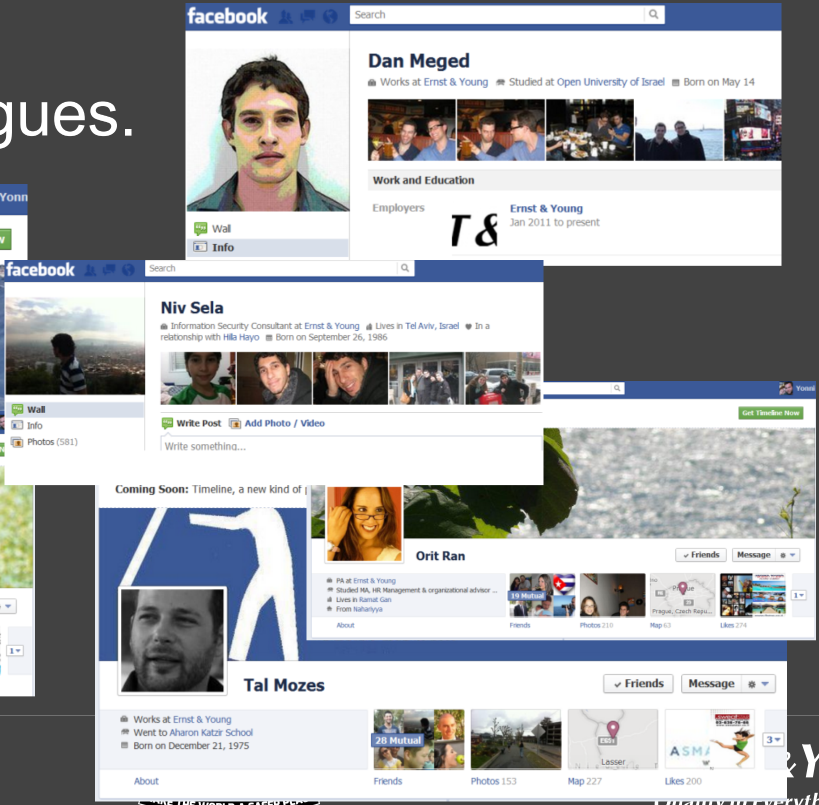
Arts and Entertainment

Music: Tiësto, Johnny Cash, Frank Sinatra, R.E.M., Ehud Banai

More

Movies

- ▶ My workplace is listed.
- ▶ Same goes for my colleagues.



Dan Meged

Works at Ernst & Young · Studied at Open University of Israel · Born on May 14

Work and Education

Employers: Ernst & Young, Jan 2011 to present

Niv Sela

Information Security Consultant at Ernst & Young · Lives in Tel Aviv, Israel · In a relationship with Hila Hayo · Born on September 26, 1986

Coming Soon: Timeline, a new kind of

Orit Ran

PA at Ernst & Young

Studied MA, HR Management & organizational advisor ...

Lives in Ramat Gan

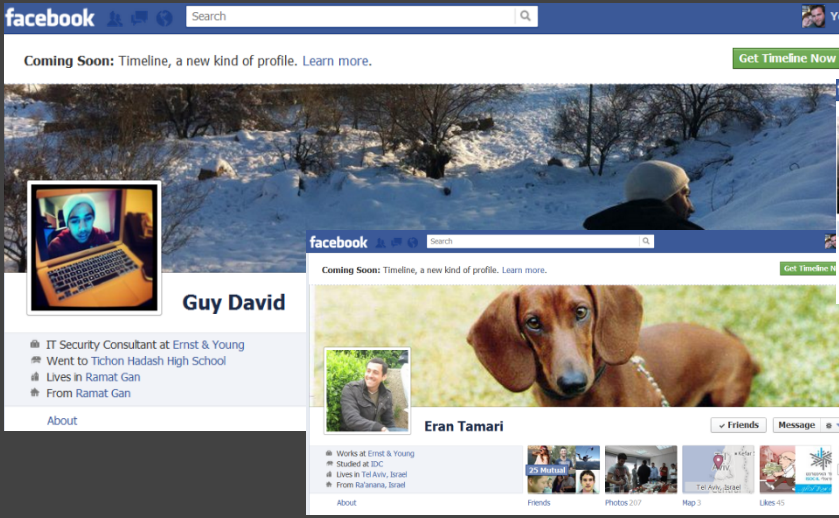
From Nahariyya

Tal Mozes

Works at Ernst & Young

Went to Aharon Katzir School

Born on December 21, 1975



Coming Soon: Timeline, a new kind of profile. Learn more.

Guy David

IT Security Consultant at Ernst & Young

Went to Tichon Hadash High School

Lives in Ramat Gan

From Ramat Gan

Eran Tamari

Works at Ernst & Young

Studied at IDC

Lives in Tel Aviv, Israel

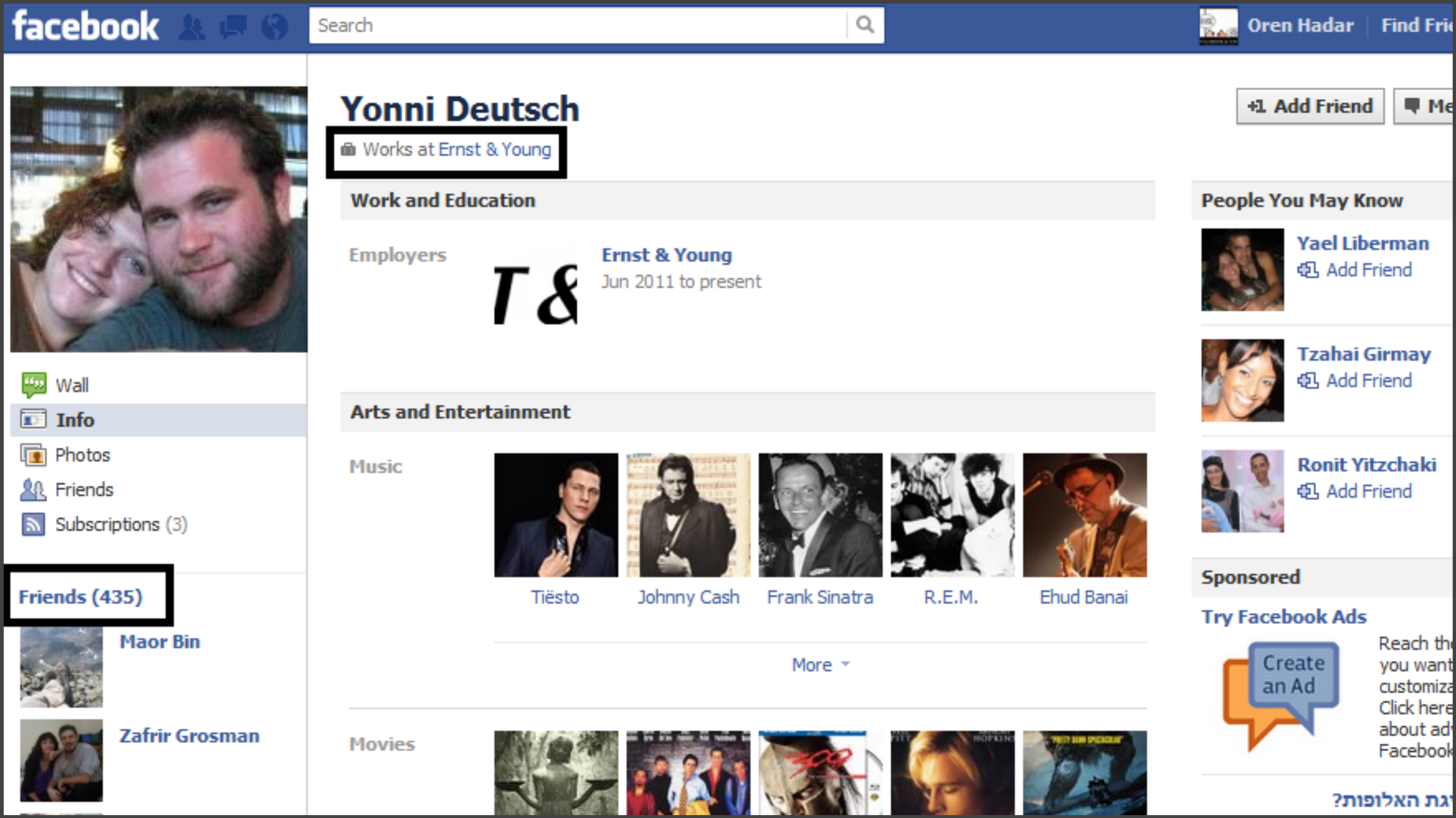
From Ra'anana, Israel

What if … ?

- We do it ourselves ?

NO SILICON
BOLD STATEMENTS
Always Best When The One Making Such Claims Is Willing To Back Their Words With Irrefutable Proof
POSTED AT
theCHIVE.com

So lets fish…



facebook

Search

Oren Hadar | Find Fri

Yonni Deutsch

Works at Ernst & Young

+1 Add Friend | Me

Wall

Info

Photos

Friends

Subscriptions (3)

Friends (435)

Maor Bin

Zafrir Grosman

Work and Education

Employers

Ernst & Young
Jun 2011 to present

Arts and Entertainment

Music

Tiësto | Johnny Cash | Frank Sinatra | R.E.M. | Ehud Banai

More ▾

Movies

People You May Know

Yael Liberman
Add Friend

Tzahai Girmay
Add Friend

Ronit Yitzchaki
Add Friend

Sponsored

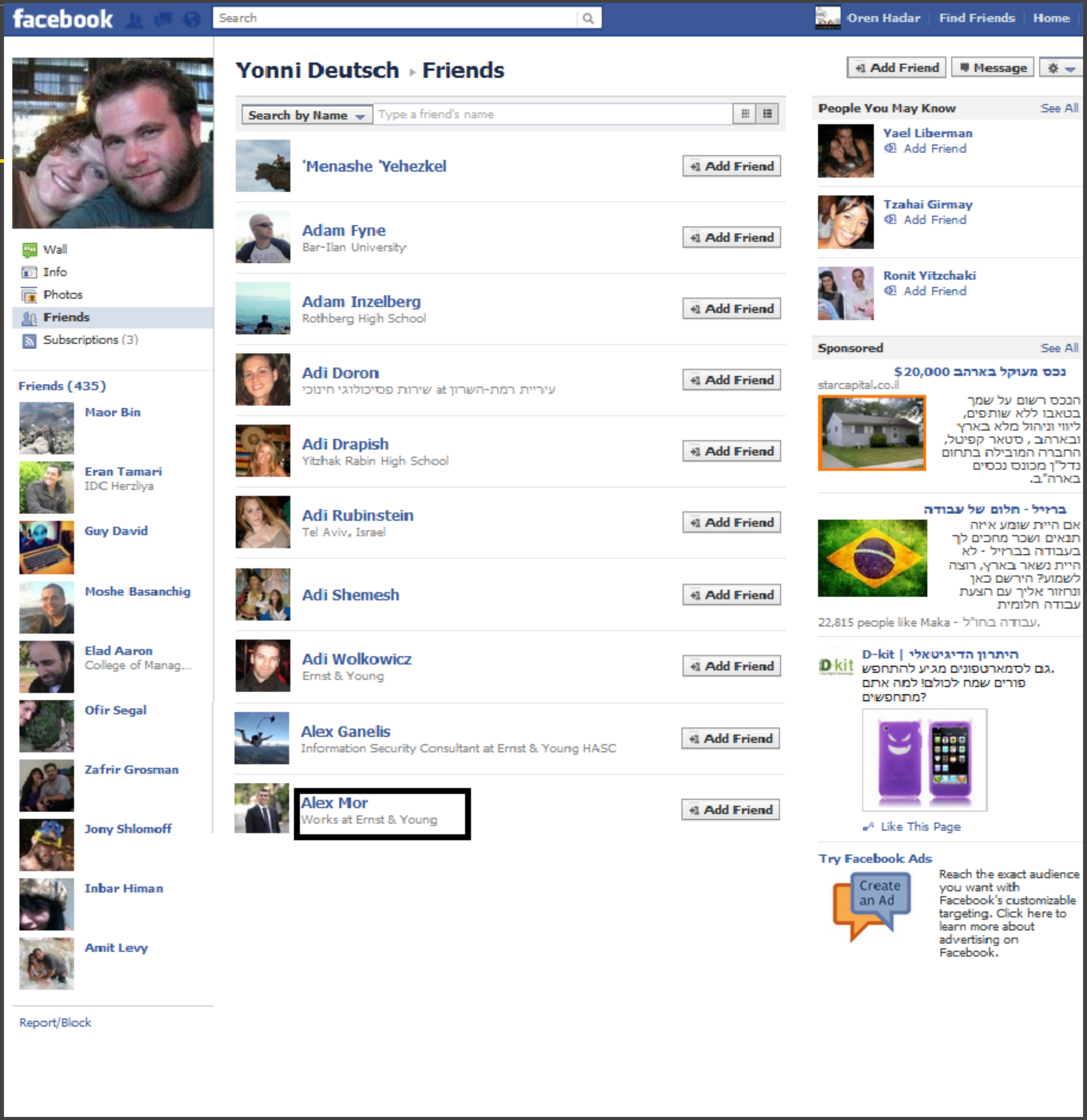
Try Facebook Ads

Create an Ad

Reach th
you want
customiza
Click here
about ad
Facebook

גת האלופות?

So lets fish…



Yonni Deutsch ▸ Friends

Friends (435)

- Maor Bin
- Eran Tamari – IDC Herzliya
- Guy David
- Moshe Basanchig
- Elad Aaron – College of Manag...
- Ofir Segal
- Zafrir Grosman
- Jony Shlomoff
- Inbar Himan
- Amit Levy

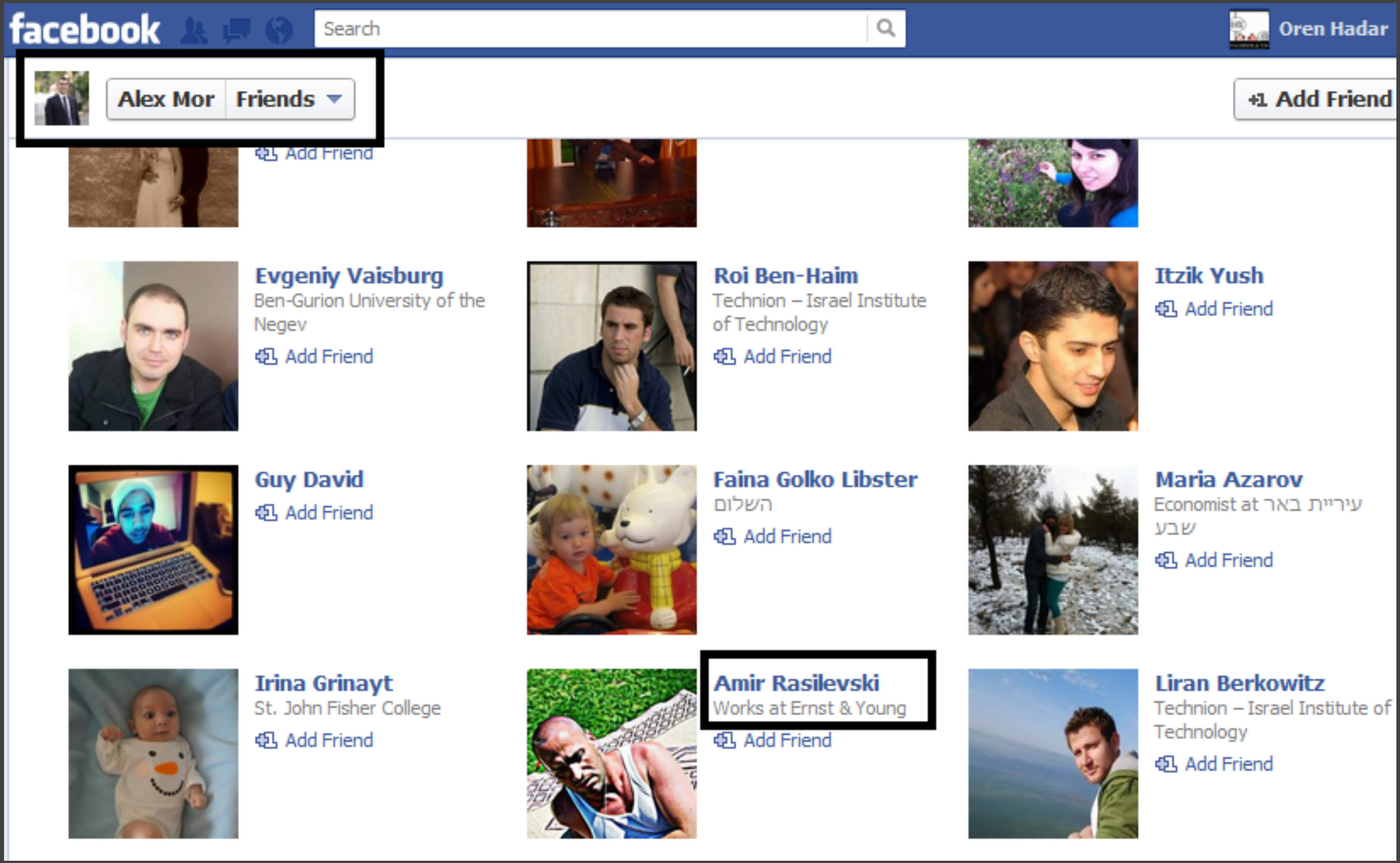
Report/Block

'Menashe 'Yehezkel	Add Friend
Adam Fyne Bar-Ilan University	Add Friend
Adam Inzelberg Rothberg High School	Add Friend
Adi Doron שירות פסיכולוגי חינוכי at עיריית רמת-השרון	Add Friend
Adi Drapish Yitzhak Rabin High School	Add Friend
Adi Rubinstein Tel Aviv, Israel	Add Friend
Adi Shemesh	Add Friend
Adi Wolkowicz Ernst & Young	Add Friend
Alex Ganelis Information Security Consultant at Ernst & Young HASC	Add Friend
Alex Mor Works at Ernst & Young	Add Friend

People You May Know — See All

- Yael Liberman – Add Friend
- Tzahai Girmay – Add Friend
- Ronit Yitzchaki – Add Friend

So lets fish…



facebook

Search

Oren Hadar

Alex Mor | Friends ▾

+1 Add Friend

Add Friend

Evgeniy Vaisburg
Ben-Gurion University of the Negev
Add Friend

Roi Ben-Haim
Technion – Israel Institute of Technology
Add Friend

Itzik Yush
Add Friend

Guy David
Add Friend

Faina Golko Libster
השלום
Add Friend

Maria Azarov
Economist at עיריית באר
שבע
Add Friend

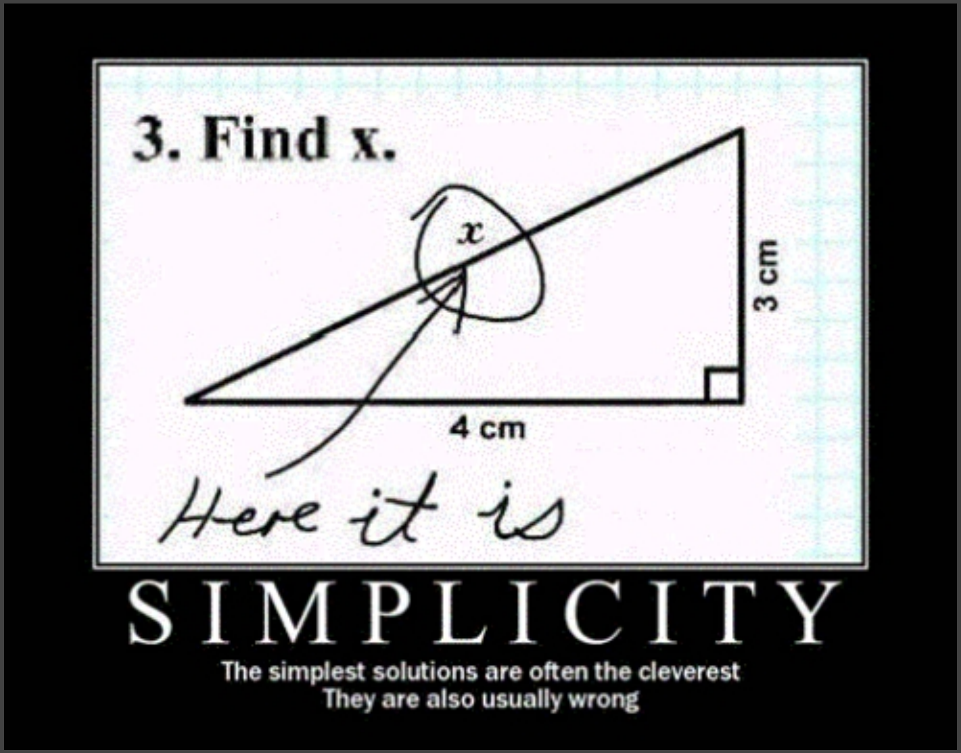
Irina Grinayt
St. John Fisher College
Add Friend

Amir Rasilevski
Works at Ernst & Young
Add Friend

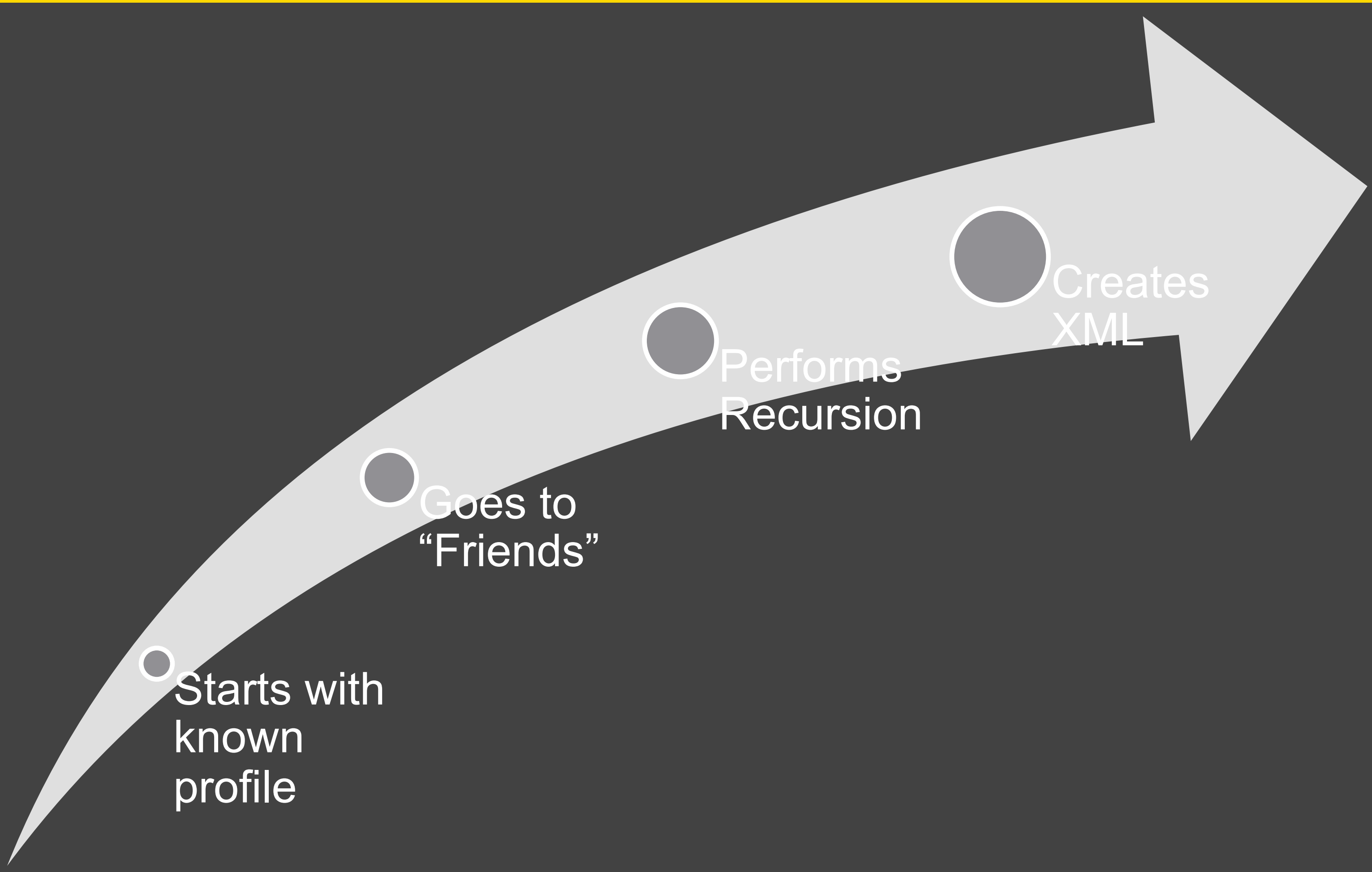
Liran Berkowitz
Technion – Israel Institute of Technology
Add Friend

If the API doesn't work…

- Sometimes, the simplest way of solving a problem, is the first one that comes to mind.


3. Find x.
x
3 cm
4 cm
Here it is
SIMPLICITY
The simplest solutions are often the cleverest
They are also usually wrong

FB Crawler in a nutshell



Starts with known profile

Goes to “Friends”

Performs Recursion

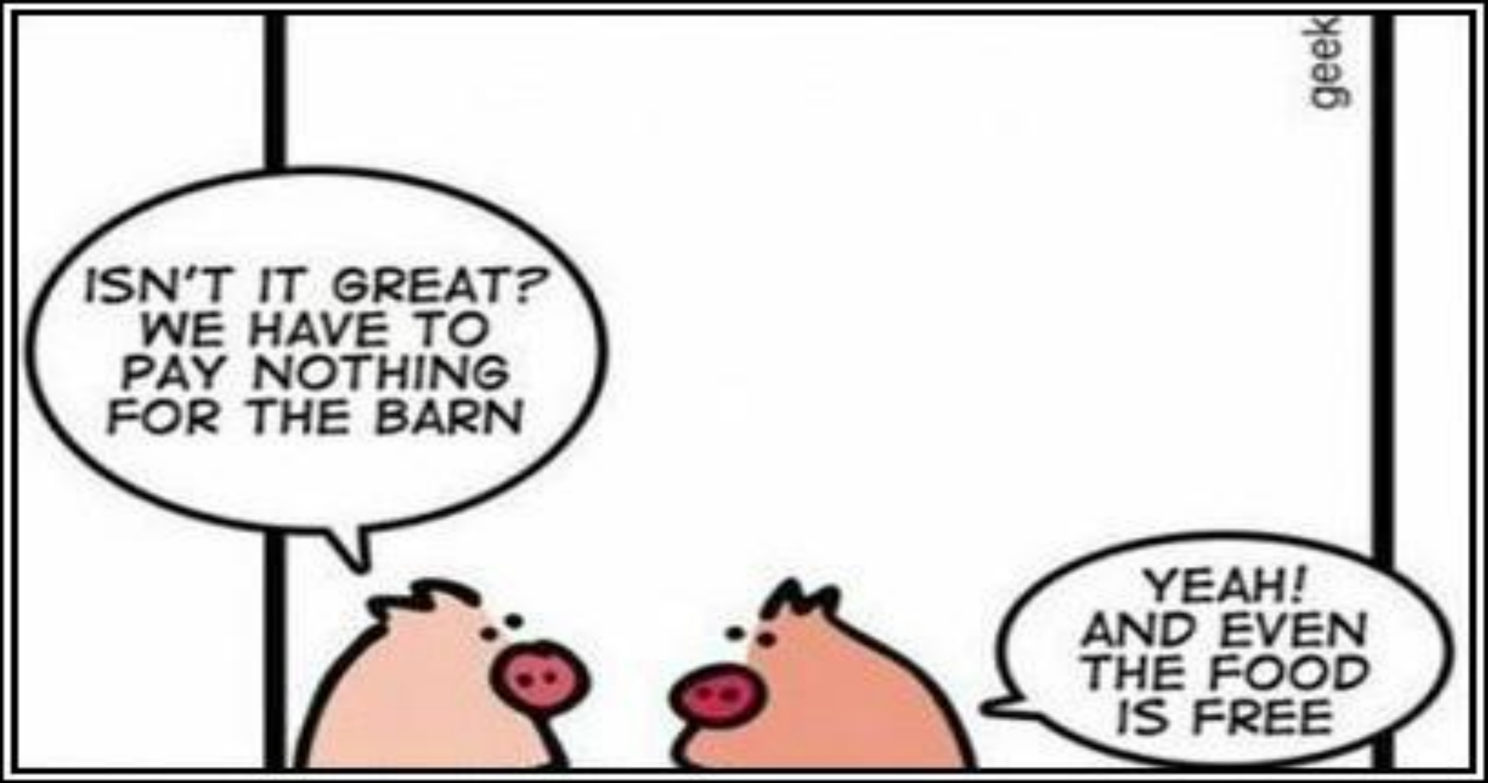
Creates XML

Meet FB Crawler

Next Steps

- Not yet graphical.
- We do use it internally and to raise awareness.

- Liability Issues.
  - Do you know what your employees are saying ?


geek
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE

FACEBOOK & YOU

If you're not paying for it, you're not the customer.
You're the product being sold