Harvesting boarding passes

28C3 – Lightning Talks – Day3

Andrei Costin <andrei@andreicostin.com>
andreicostin.com/papers

Intro

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA 616 OCT 14
FROM SEATTLE
TO CHICAGO/OHARE
GATE N13
DEPARTS AT 7:28 AM
GIVE FEEDBACK - WWW.UALSURVEY.COM
SEAT 7A
Y-CABIN
** PAPER REQUIRED **

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA 688 OCT 14
FROM CHICAGO/OHARE
TO NYC/LAGUARDIA
GATE B7
DEPARTS AT 4:05 PM
GIVE FEEDBACK - WWW.UALSURVEY.COM
SEAT 1C
F-CABIN
** PAPER REQUIRED **

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA7371 OCT 21
FROM NYC/LAGUARDIA
TO WASH/DULLES
GATE C7
DEPARTS AT 7:00 AM
GIVE FEEDBACK - WWW.UALSURVEY.COM
SEAT 1C
Y-CABIN
** PAPER REQUIRED **

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
SA 208 OCT 21
FROM WASH/DULLES
TO JOHANNESBURG
GATE IAD
DEPARTS AT 12:50 PM
SEAT 3H
78
C-CABIN
** PAPER REQUIRED **

FLIGHT: 1T 110	DATE: 08/11
SEAT: 4C	DESTINATION: JNB
GATE: 16	BOARDING TIME: 15h05

BOARDING GATES CLOSE 20 MINUTES PRIOR TO DEPARTURE

BUSINESS 329
TRIPP/KIMBERLY L M
JNB
FRA
LUFTHANSA UA*G
LH 573 C 03NOV
008 2015 2B
MK
swissport

BUSINESS 149
Bordkarte/Boarding Pass
TRIPP/KIMBERLY L M
FRA
BCN
LUFTHANSA UA*G
LH 4452 C 08NOV
08 0520 6K
NONSMOKER

BRITISH AIRWAYS
TRIPP/KIMBERLYL
BA/BLUE13294604
BARCELONA BCN
LONDON LHR
BA 477 C 08NOV 0735
51 0715 SEAT 03A XX
0 0 0 009
PASSENGER TICKET AND BAGGAGE CHECK
** ETKT

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA 935 NOV 8
FROM LON / HEATHRO
TO LOS ANGELES
DEPARTS AT 11:15 AM
BOARDS AT 10:30 AM
SEAT 12H
C-CABIN
016 2147179137 CPN 1

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA1519 NOV 8
FROM LOS ANGELES
TO LAS VEGAS
DEPARTS AT 5:00 PM
BOARDS AT 4:30 PM
SEAT 1C
Y-CABIN
016 2147179137 CPN 2

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA1425 NOV 11
FROM LAS VEGAS
TO SAN FRANCISCO
GATE D55
DEPARTS AT 8:38 AM
BOARDS AT 8:08 AM
SEAT 3C
Y-CABIN
016 2149768343 CPN 1

TRIPP/KIMBERLYLMRS
PREMIER EXEC 100K
UA 00305949370
UA 930 NOV 11
FROM SAN FRANCISCO
TO LON / HEATHRO
DEPARTS AT 12:30 PM
BOARDS AT 11:45 AM
SEAT 15H
C-CABIN
016 2149768343 CPN 2

BRITISH AIRWAYS
TRIPP/KIMBERLYL
BA/BLUE13294604
LONDON LHR
BARCELONA BCN
BA 478 M 12NOV 0725
26 0715 SEAT 18A XX
0 0 0 169
PASSENGER TICKET AND BAGGAGE CHECK
X2 ETKT NO COUPON

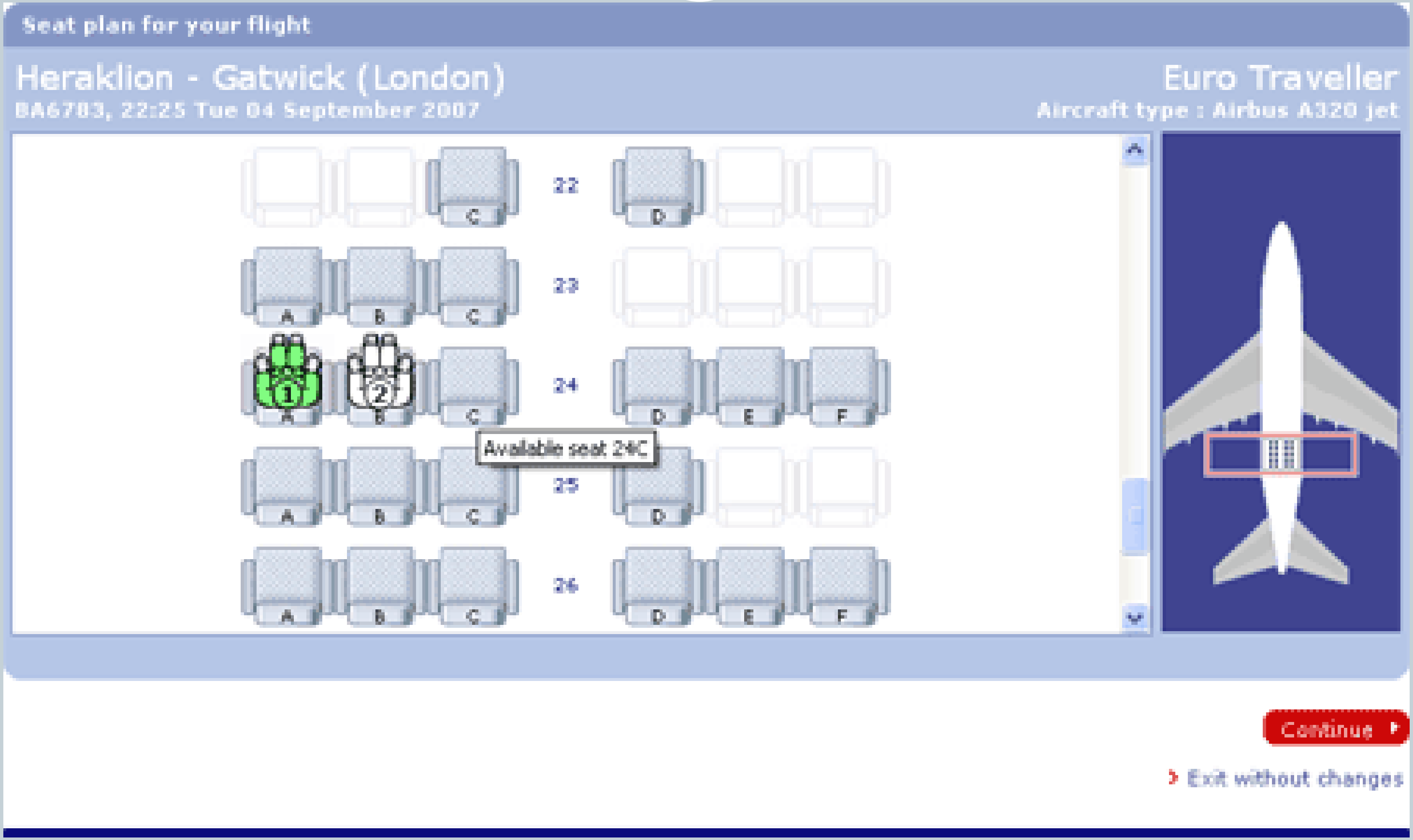
BUSINESS 029
Bordkarte/Boarding Pass
TRIPP/KIMBERLY L M
BCN
FRA
LUFTHANSA UA*G
LH 4465 C 18NOV
032 0630 XXXXXXX
3C
NONSMOKER

BUSINESS 328
Bordkarte/Boarding Pass
API
TRIPP/KIMBERLY L M
FRA
IAD
UNITED AIRLINES UA*G
UA 917 C 18NOV
1140 16A
NONSMOKER

BUSINESS 137
Bordkarte/Boarding Pass
TRIPP/KIMBERLY L M
IAD
SEA
UNITED AIRLINES UA*G
UA 917 C 18NOV
1635 7B
NONSMOKER

Modern concerns

Online check-in is established trend



Seat plan for your flight

Heraklion - Gatwick (London)

BA6783, 22:25 Tue 04 September 2007

Euro Traveller

Aircraft type : Airbus A320 jet

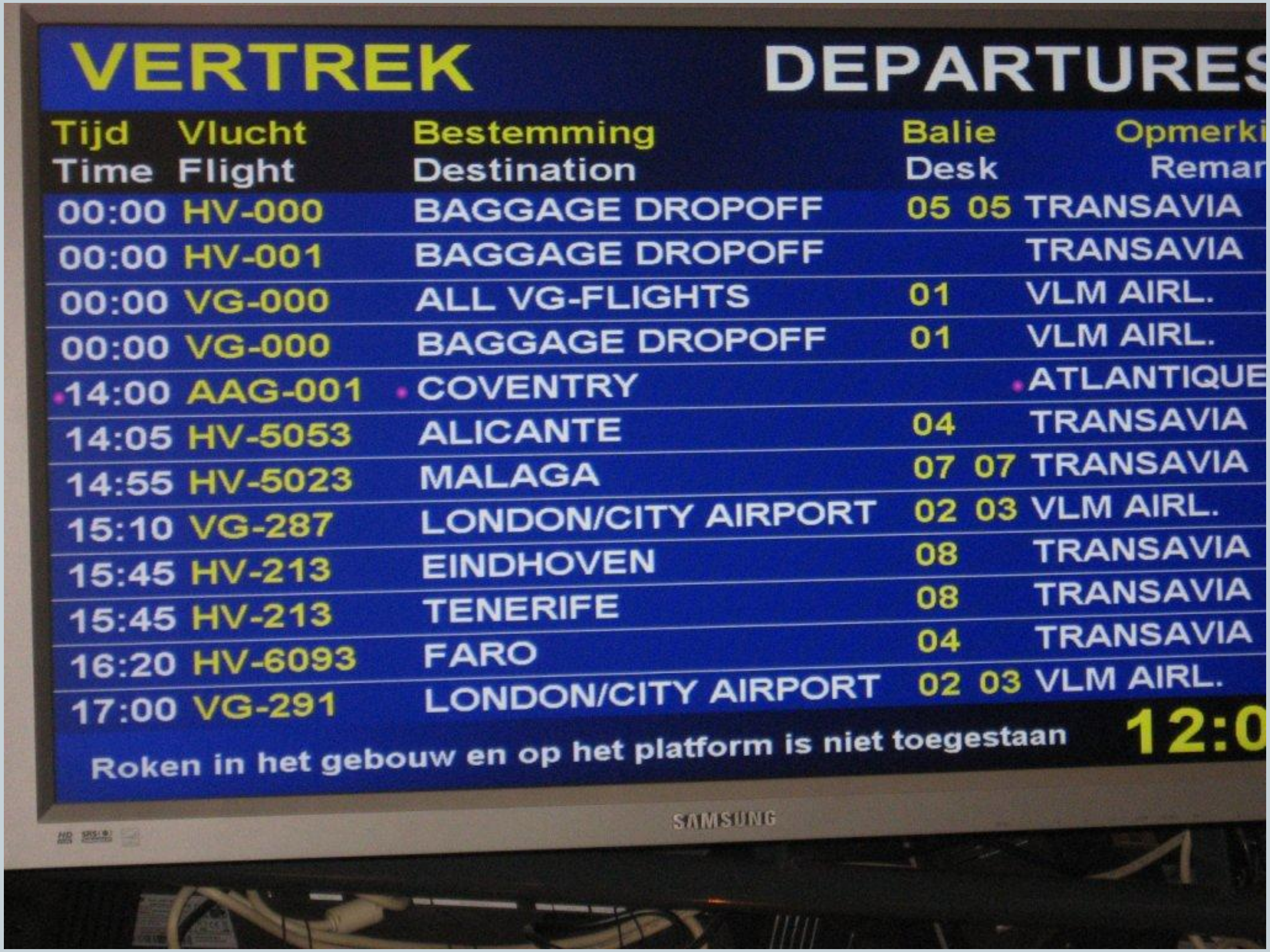
Available seat 24C

We can learn airline preferences

UNITED
AIR CANADA
AMERICA WEST
U·S AIRWAYS
CATHAY PACIFIC
AmericanAirlines
BRITISH AIRWAYS
ANA
Alitalia
sabena
AIR FRANCE
virgin atlantic
QANTAS
JAL
Delta Air Lines
AIR NEW ZEALAND
NORTHWEST
VARIG
Lufthansa
Thai
Thai Airways International
swissair
SINGAPORE AIRLINES
SAS
KLM

FTdetails – checkins, logins, other actions

Preferred hours – predictable time

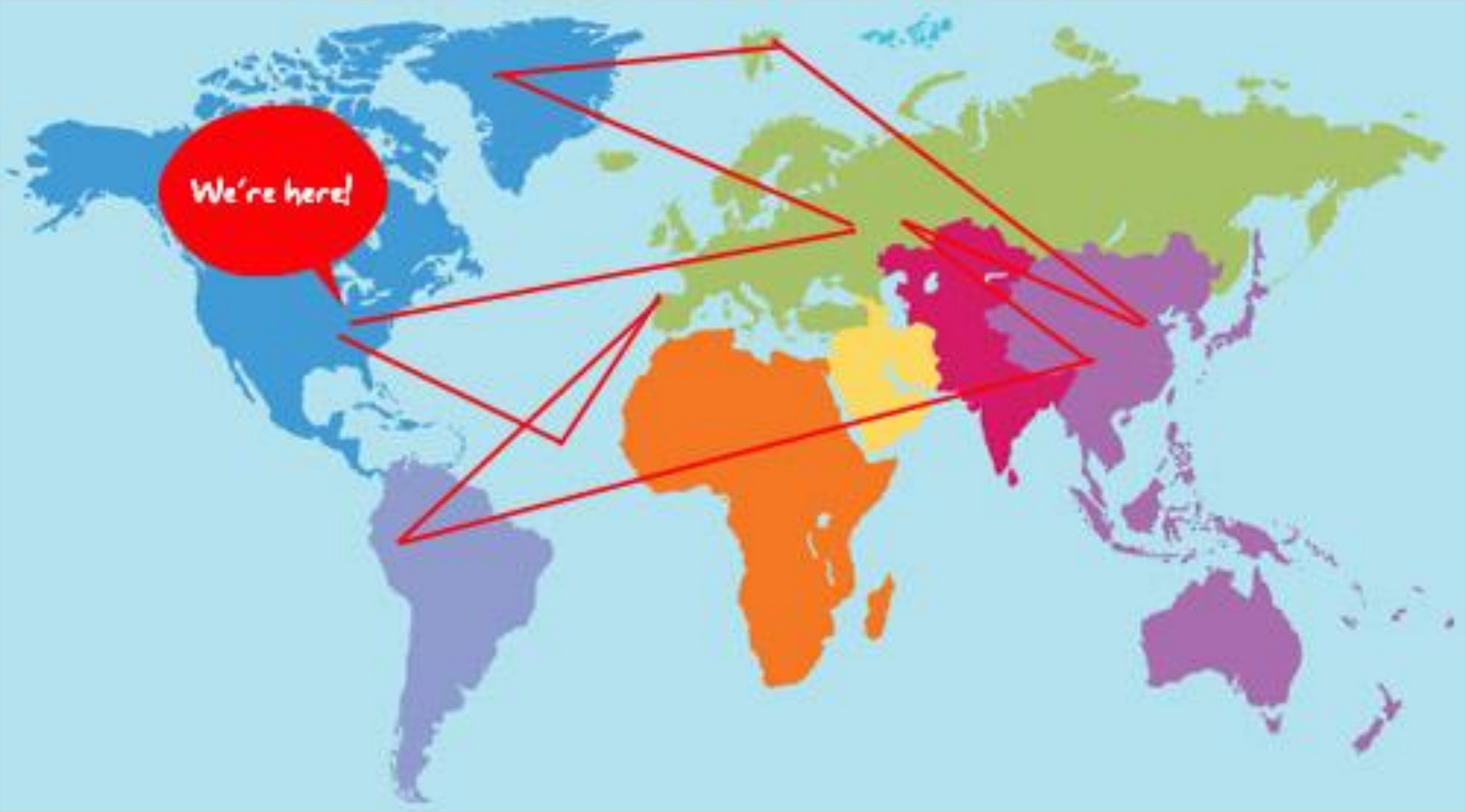


VERTREK DEPARTURES

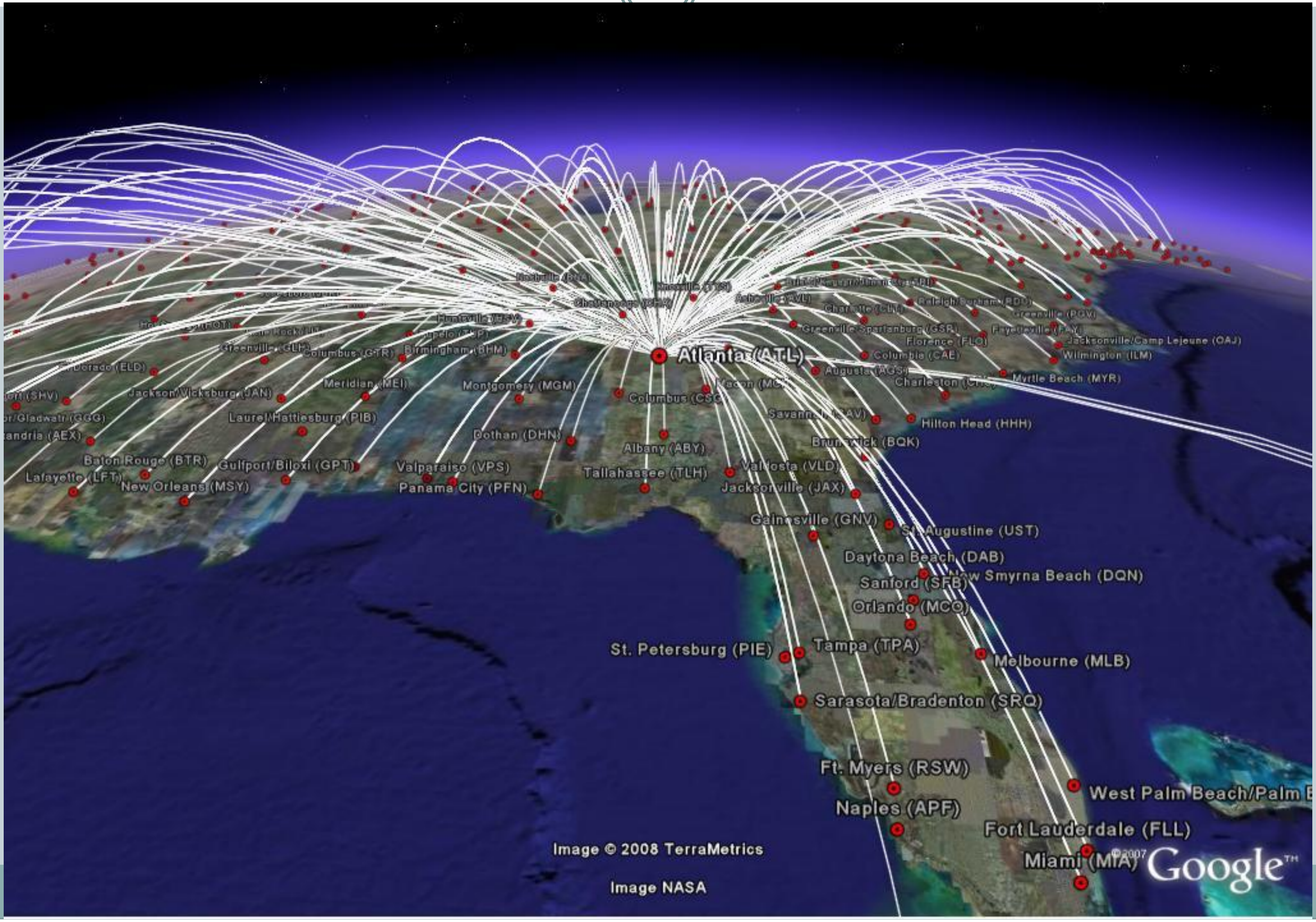
Tijd Time	Vlucht Flight	Bestemming Destination	Balie Desk	Opmerki Remar
00:00	HV-000	BAGGAGE DROPOFF	05 05	TRANSAVIA
00:00	HV-001	BAGGAGE DROPOFF		TRANSAVIA
00:00	VG-000	ALL VG-FLIGHTS	01	VLM AIRL.
00:00	VG-000	BAGGAGE DROPOFF	01	VLM AIRL.
14:00	AAG-001	COVENTRY		ATLANTIQUE
14:05	HV-5053	ALICANTE	04	TRANSAVIA
14:55	HV-5023	MALAGA	07 07	TRANSAVIA
15:10	VG-287	LONDON/CITY AIRPORT	02 03	VLM AIRL.
15:45	HV-213	EINDHOVEN	08	TRANSAVIA
15:45	HV-213	TENERIFE	08	TRANSAVIA
16:20	HV-6093	FARO	04	TRANSAVIA
17:00	VG-291	LONDON/CITY AIRPORT	02 03	VLM AIRL.

Roken in het gebouw en op het platform is niet toegestaan 12:0

Preferred routes/ports – predictable space



Predictable $HOME



Various /dev/random ideas

- Track reconstruction/following
  - and eventually analysis and alarm in case out-of-pattern/out-of-plan actions occur
- Learn travelling habits
  - so that next “moves” can be predicted/evaluated and attacker-actions planned accordingly, etc.

Various /dev/random ideas

- Impersonate the person with a higher degree of credibility given level of details learned
- Learn very-near future plans
  - every 24h window try to check-in given FT-number and last name and see what flights are scheduled for the person)

Various /dev/random ideas

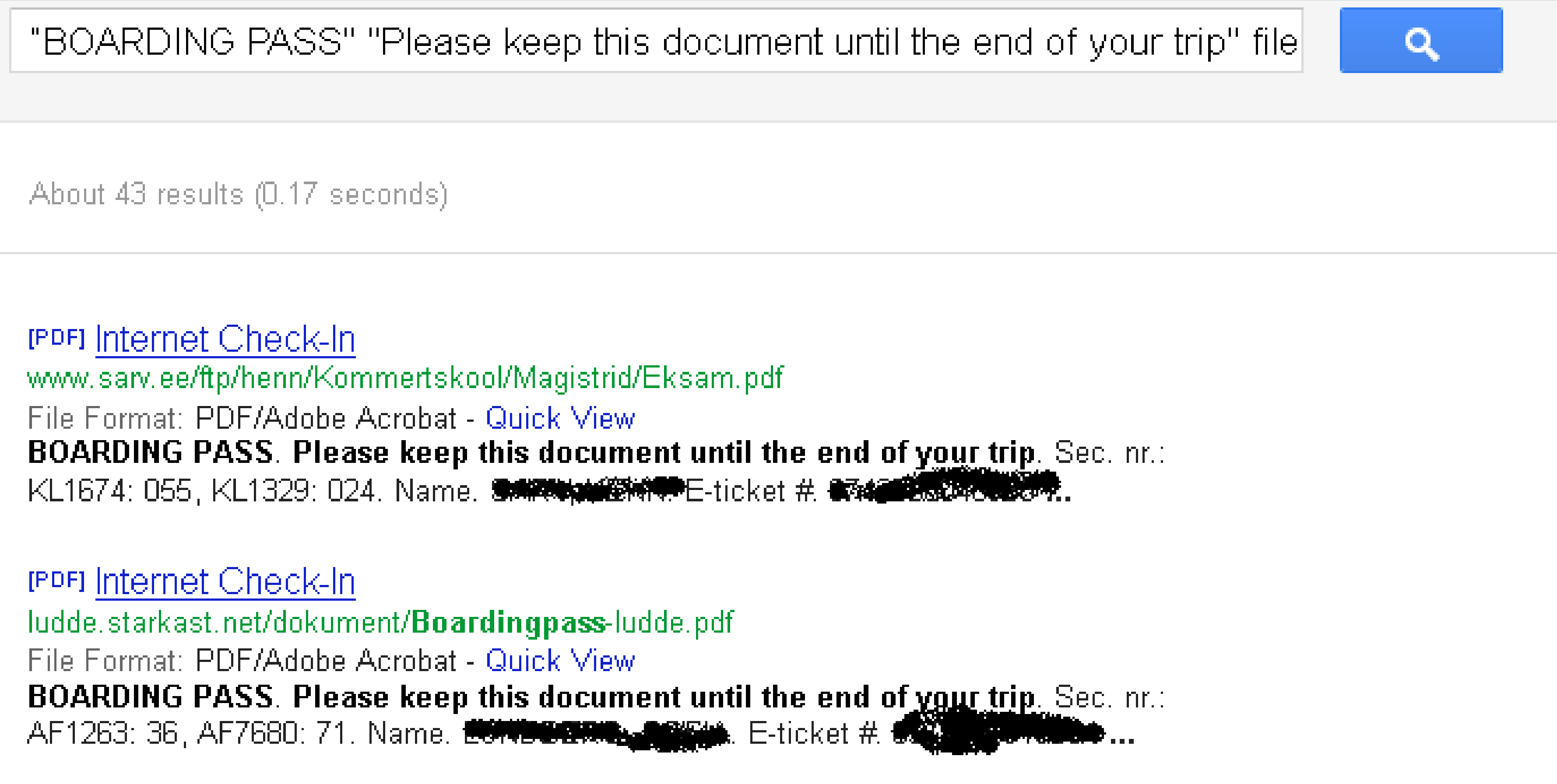
- Direct effects on victim’s plans
  - checkin cancelation
  - checkin seat-assignment convenient to the attacker so that next-phases of social engineering can be conducted
  - group-checkin impersonation so that person is being more or less associated with a group of persons (good or bad) without their own will

Various /dev/random ideas

- Marriage cheating cases more easily detectable, etc.
  - Useful for private-detective services

- Deliberate “leakage” of fake/misleading boarding passes by the “victim”
  - “victim” is actually an attacker in this case
  - so that intelligence gathering dudes will have a hard time tracking down the so called “victim” ☺

Useful "google dorks"



"BOARDING PASS" "Please keep this document until the end of your trip" file

About 43 results (0.17 seconds)

[PDF] Internet Check-In
www.sarv.ee/ftp/henn/Kommertskool/Magistrid/Eksam.pdf
File Format: PDF/Adobe Acrobat - Quick View
BOARDING PASS. **Please keep this document until the end of your trip**. Sec. nr.: KL1674: 055, KL1329: 024. Name. [redacted] E-ticket #. [redacted]..

[PDF] Internet Check-In
ludde.starkast.net/dokument/**Boardingpass**-ludde.pdf
File Format: PDF/Adobe Acrobat - Quick View
BOARDING PASS. **Please keep this document until the end of your trip**. Sec. nr.: AF1263: 36, AF7680: 71. Name. [redacted]. E-ticket #. [redacted] ...

Useful “google dorks”

- KLM
  - “BOARDING PASS" "Please keep this document until the end of your trip" filetype:pdf
  - intitle:"Internet Check-In" filetype:pdf
  - "Internet-CheckIn-Boarding-Docs.pdf“
- LUFTHANSA
  - "API+Boarding+Pass"+filetype:pdf
  - (name OR nome) "etix" "Boarding Pass" filetype:pdf
  - boarding pass etix intitle:lufthansa intitle:pdf filetype:pdf

Useful “google dorks”

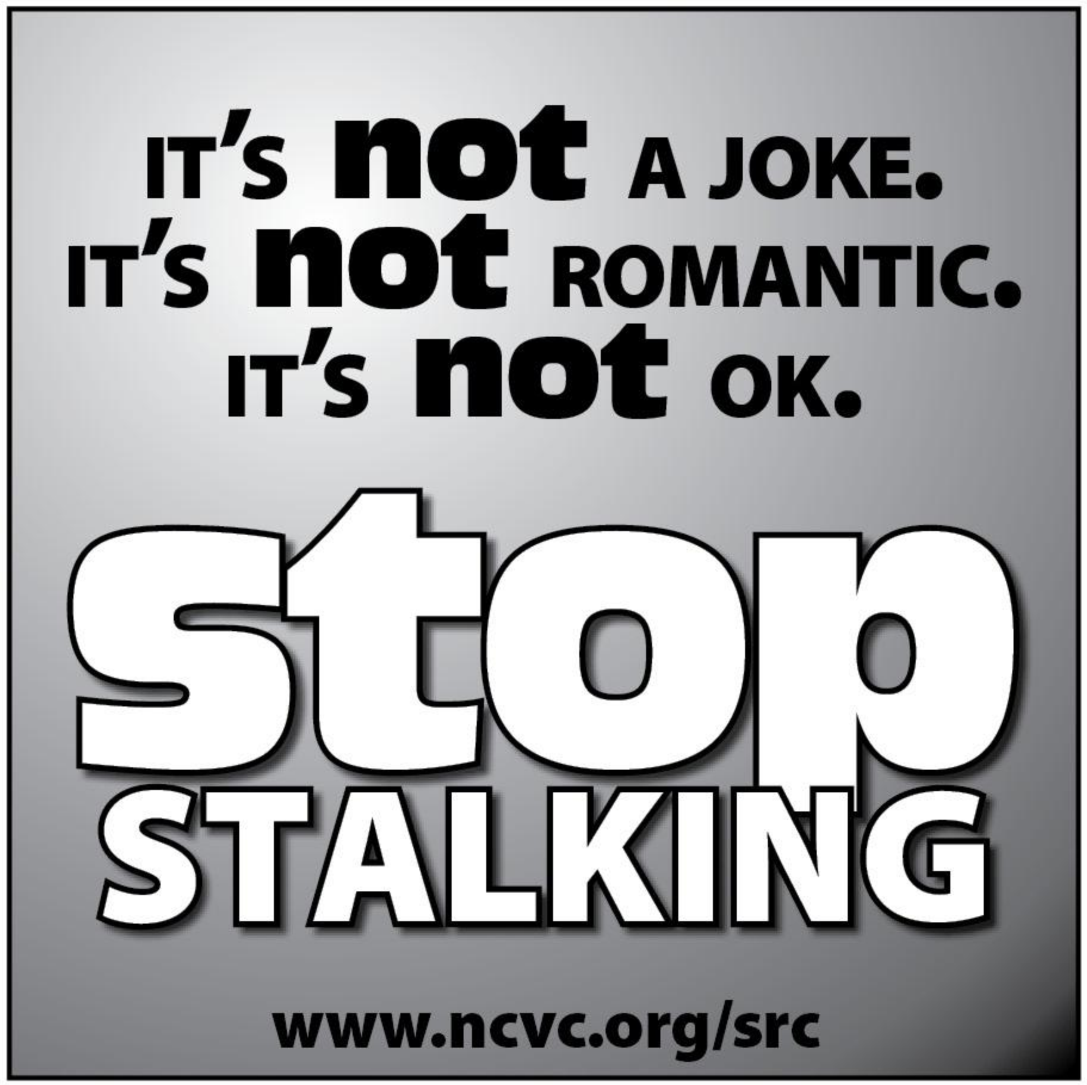
- AMERICAN AIRLINES
  - "Print+Boarding+Pass(es)“
- EASYJET
  - "easyJet.com Internet check-in boarding pass" filetype:pdf
- AEGEAN
  - "boardingPass.pdf“
- JETSTAR
  - "Web Check-in Boarding Pass" filetype:pdf

Take away: secure your sensitive details

Take away: Contribute

- http://www.exploit-db.com/google-dorks/

Take away: Don’t stalk!



IT’S **not** A JOKE.
IT’S **not** ROMANTIC.
IT’S **not** OK.

stop
STALKING

www.ncvc.org/src

Thanks

- andrei@andreicostin.com
- andreicostin.com/papers
- Harvesting boarding passes