

Project Topic:

Visual Summaries of Analyses  
from Log Data

# Visual Summaries from Log Data

- Difficult to understand human analysis processes for collaboration and presentation
- Analysts don't want to record their thoughts
- Can we automate visual summaries of an analysis?

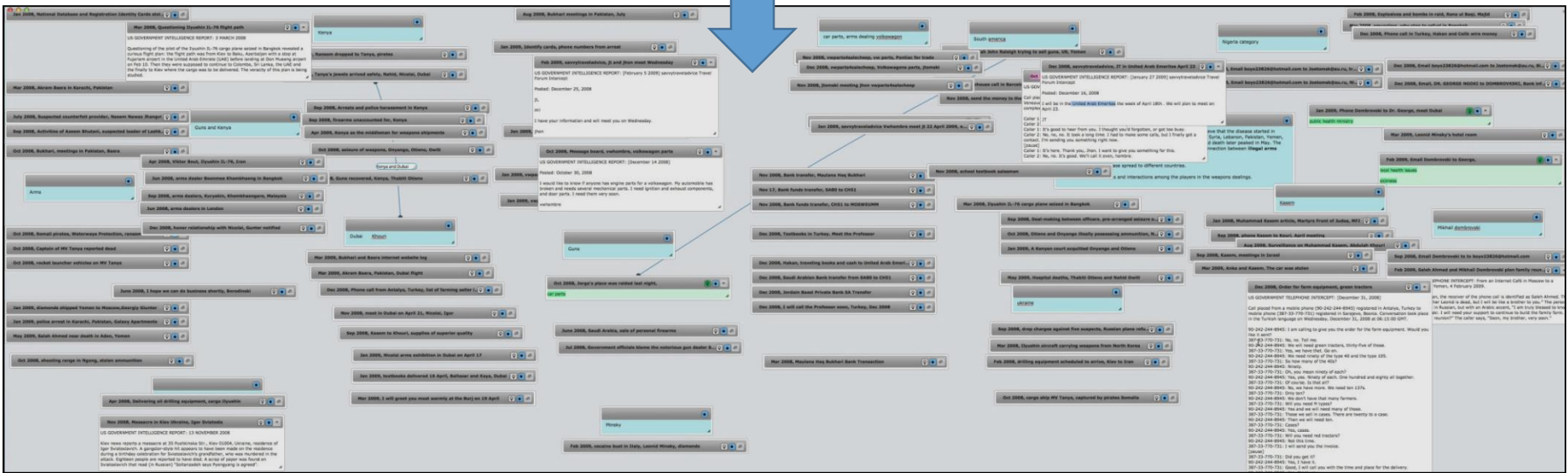


# Visual Summaries from Log Data

- Background:
  - Human exploration of data is complicated
  - Supporting human data analysis requires understanding human analysis behaviors and patterns
  - Explaining strategies is difficult
- Goal:
  - Generate visual summaries of human data analysis behavior by using system event logs from analysis tools



Jan 2006, National Database and Registration Identity Cards shot	Aug 2006, Email buys23826@hotmail.com to Jastrom@du.ru, Ir	Feb 2006, drilling equipment scheduled to arrive, Kiev to Iran	Dec 2006, Phone call in Turkey, Hakan and Gail's wife money
Mar 2006, Questioning Tsyapkin SL-76 flight path	Oct 2006, Email buys23826@hotmail.com to Jastrom@du.ru, Ir	Mar 2006, Huseina Hag Babukali Bank Transaction	Oct 2006, Email buys23826@hotmail.com to Jastrom@du.ru, Ir
Mar 2006, Tsyapkin SL-76 cargo plane seized in Bangkok	Oct 2006, Email buys23826@hotmail.com to Jastrom@du.ru, Ir	June 2006, I hope we can do business shortly, Boroedini	Jan 2007, textbooks delivered 16 April, Balasaur and Kava, Dubai
Apr 2006, Visitor Road, Tsyapkin SL-76, Iran	June 2006, Baskali and Baska internet website log	Dec 2006, Kaseen to Kheuri, supplies of superior quality	Mar 2007, I will grant you most warmly at the Burj on 19 April
Jun 2006, arms dealer in London	June 2006, Baskali, sale of personal weapons	Oct 2006, Isayev's phone was called last night, gun parts, guns	Apr 2006, Tsyapkin's private aircraft safety, Beirut, Moscow, Dubai
Mar 2006, Aliman Baska in Karachi, Pakistan	Nov 2006, Arsenals and police harassment in Karsya	Oct 2006, Isayev I have a birthday present for you	Jan 2006, Mohammed Kaseen article, Marjory Frost of Dubai, M93
Jun 2006, arms dealer Rusevina Khoshkhaev in Bangkok	Dec 2006, Email buys23826@hotmail.com to Jastrom@du.ru, Ir	Oct 2006, warehouse call in Barcelona, Venezuela	Feb 2006, Explosives and bombs to raid, Base of Raed, Raed
Jul 2006, Russian counterfeiter president, Nassim Nassim Zheng	Dec 2006, Insurance cancelled for Karsya	Dec 2006, phone Kaseen to Kheuri, April meeting	Mar 2006, Tsyapkin aircraft carrying weapons from North Korea
Dec 2006, Activities of Isayev Baskali, suspected leader of Lash	Oct 2006, shooting clinic in Nigeria, stolen ammunition	Nov 2006, used the money to the Green Men	Mar 2006, smuggler, why stop to reflect in Bangkok
Dec 2006, weapons of Isayev Baskali, suspected leader of Lash	Nov 2006, weapons of weapons, Dnyanyan, Oltene, Oltene	Jan 2006, where textbook salesman	Apr 2006, Delivering oil drilling equipment, cargo Dnyanyan
Aug 2006, arms dealer, Karyukhin, Khoshkhaev, Malaysia	Mar 2006, Isayev dropped by Tsyapkin, private	Nov 2006, Isayev in Dubai on April 22, Moscow, Iran	May 2006, Tsyapkin John Ralston trying to sell guns, US, Yemen
Aug 2006, Isayev/Isayev on Mohammed Kaseen, Ralston Khuri	Apr 2006, Karsya as the midwives for weapons shipments	Nov 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Jul 2006, Government officials blame the unknown gun dealer R
Oct 2006, Kaseen recovered, Kaseen, Tsyapkin Oltene	Dec 2006, Order for farm equipment, guns brokers	Nov 2006, Jastrom meeting Isayev Isayev	Dec 2006, drop charges against five Russians, Russian phone calls
Oct 2006, Baskali, meetings in Pakistan, Baska	Mar 2006, Isayev and Kaseen. The car was stolen	Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Mar 2006, Lashin Misha's hotel room
Oct 2006, cargo ship MY Tanya, captured by pirates Somalia		Feb 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Dec 2006, Isayev meeting Baskali, Isayev meeting Jastrom, Arab Gulf
Dec 2006, Isayev, meetings in Israel		Jan 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Oct 2006, Oltene and Dnyanyan Isayev possessing ammunition, M
Oct 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Jan 2006, A Kaseen court acquitted Dnyanyan and Oltene
Oct 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Feb 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf
Nov 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	Mar 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf
Jan 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	May 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf
Mar 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	
Jan 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	
May 2006, Isayev, Isayev, Isayev, Isayev, Isayev		Dec 2006, Isayev to Baskali, Isayev meeting Jastrom, Arab Gulf	





**Mar 2009, Leonid Minsky's hotel room**

Report Date: 10 March 2009 from the New York Times

The scene is Leonid Minsky's hotel room on the night of February 1, 2009. Minsky is a tall, pale and fat and of Ukrainian origin. He is surrounded by Ukrainian prostitutes. Minsky is in a small town outside of Kyiv, in a hall, and a hangout of shady characters. They arrive at Room 341, putting up a prominent international gun. Minsky was reportedly shot to death in the room. The room is sketchy.

Minsky is a tip from an unpaid prostitute, customs police had had Minsky. Minsky is a prominent international criminal organization. The foreign bank accounts of Minsky are linked to Italian intelligence services. Minsky is of Ukrainian origins associated with a network of international arms and drug trafficking, money laundering, extortion and other offenses. A key leader in this organization is Minsky.

That hot August evening in Soncino, police found \$500,000 worth of uncut diamonds. Later analysis found most came from Russia -- no African origins could be confirmed despite the diamond scales later found in Minsky's Lagos office. They found receipts for diamond and gun shipments to Yemen. They found a duffel bag filled with more than \$35,000 in American, Italian, Hungarian and Mauritian currency. From a briefcase and piles scattered around the rooms, police collected 1,500 documents -- in Russian, Ukrainian, French, German, Dutch, English and Italian -- relating to Minsky's wide variety of business operations. Specific findings included documents on his dealings in oil, timber and consumer goods; maps of the Kenya-Sudan border; an inquiry by Minsky concerning Nigerian civil engineering and bridge construction services; an offer from Minsky's Korean representative asking him to ascertain whether Liberian President Charles Taylor would be interested in establishing diplomatic relations with Pyongyang; and a record of a \$30,333.23 payment to Anna Nicole Smith as "a thank you and an apology." Most important, however, police found evidence of several proposed and realized arms deals.

**Dec 2008, Phone call in Turkey, Hakan and Celik wire money**

US GOVERNMENT TELEPHONE INTERCEPT: [December 3, 2008]

Call placed from a mobile phone (90-242-244-8945) registered in Antalya, Turkey to mobile phone (90-0212-516-90-24) registered in Istanbul, Turkey. Conversation took place in the Kurmanji language on Wednesday, December 3, 2008 at 14:05:00 GMT.

90-242-244-8945: Hakan, we are close to making a deal with- [pause] with our contact. When can you have the money ready?

90-0212-516-90-24: I can have it ready in two weeks. You must give me three days notice, however, if you want to have it in cash. If you want the money wired, I can arrange that within 24 hours. You must not forget, Celik.

90-242-244-8945: Good. I will call you as soon as we know.

**Jan 2009, vwparts4salecheep, Jhon meeting jtomski, Arab Sail**

payment and shipment

Arab Sail in April

jtomski

**dealers in London**

INTELLIGENCE REPORT: June 9, 2008 from M15

Two suspected arms dealers Nicolai Kuryakin and Boonmee are registered attendees at the Defence Systems Equipment Conference in London that began on June 7, 2008.

**Feb 2009, cocaine bust in Italy, Leonid Minsky, diamonds**

Report Date: 2 February 2009 from La Repubblica (Italy)

Rome -- A recent cocaine bust in Italy turned into a surprise of international intrigue. Italian police discovered four prostitutes in a hotel room with a Ukrainian businessman named Leonid Minsky. The police also discovered more than \$35,000 in cash, a half-million dollars in diamonds, and more than 1,500 documents detailing a tangled web of business dealings in oil, diamonds, and gun shipments to Yemen. Two days after Minsky was placed in custody, he was found dead in his cell due to unknown cause. Florence police are being supported in their investigation by UN arms experts.

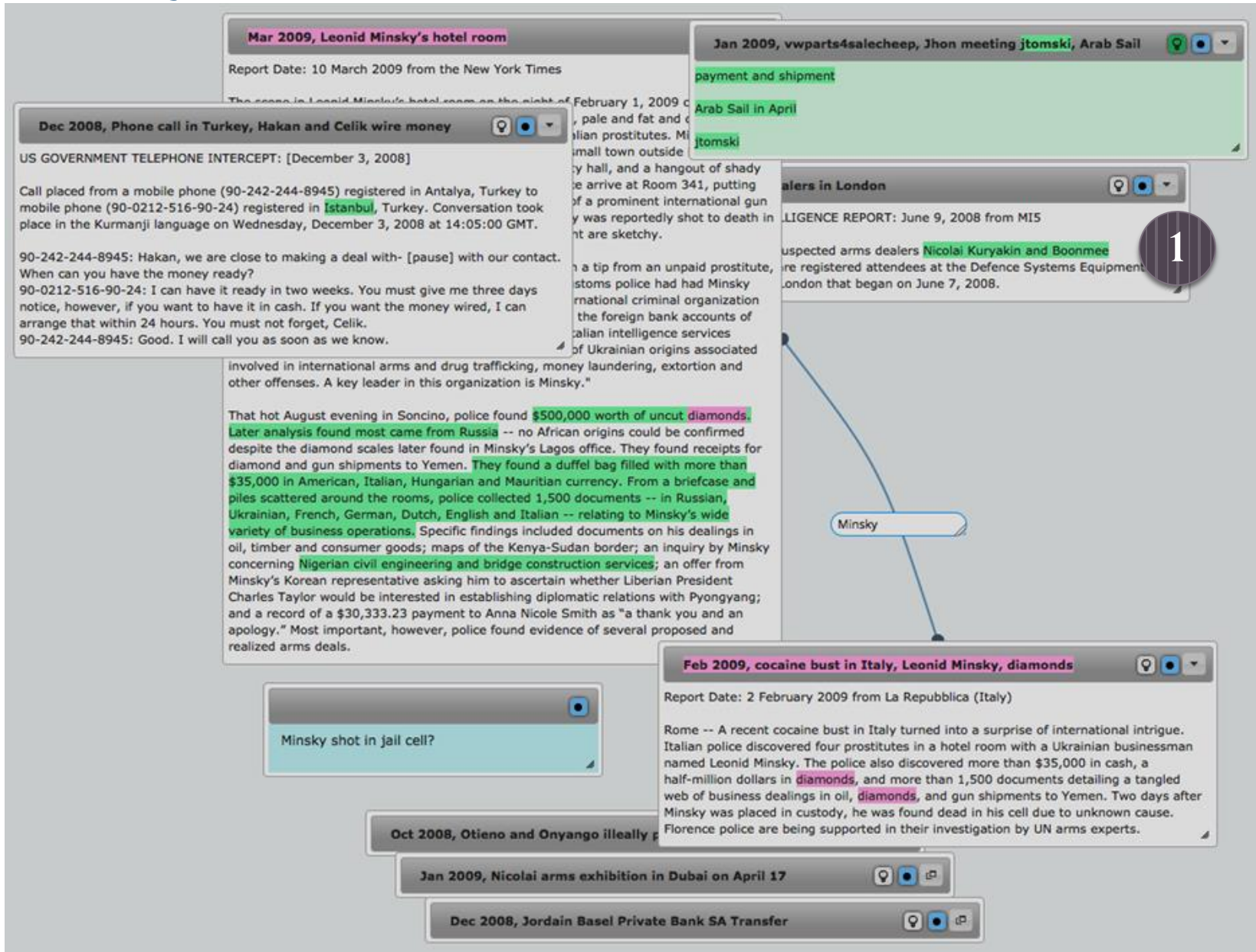
**Oct 2008, Otieno and Onyango illegally**

**Jan 2009, Nicolai arms exhibition in Dubai on April 17**

**Dec 2008, Jordain Basel Private Bank SA Transfer**

Minsky

# History of Data Interaction





# History of Data Interaction

2

Mar 2009, Leonid Minsky's hotel room

Report Date: 10 March 2009 from the New York Times

The scene in Leonid Minsky's hotel room on the night of

February 1, 2009 c  
pale and fat and c  
sian prostitutes. Mi  
small town outside  
y hall, and a hangout of shady  
e arrive at Room 341, putting  
of a prominent international gun  
y was reportedly shot to death in  
nt are sketchy.

h a tip from an unpaid prostitute,  
stoms police had had Minsky  
ernational criminal organization  
the foreign bank accounts of  
alian intelligence services  
of Ukrainian origins associated

involved in international arms and drug trafficking, money laundering, extortion and other offenses. A key leader in this organization is Minsky."

That hot August evening in Soncino, police found \$500,000 worth of uncut diamonds. Later analysis found most came from Russia -- no African origins could be confirmed despite the diamond scales later found in Minsky's Lagos office. They found receipts for diamond and gun shipments to Yemen. They found a duffel bag filled with more than \$35,000 in American, Italian, Hungarian and Mauritian currency. From a briefcase and piles scattered around the rooms, police collected 1,500 documents -- in Russian, Ukrainian, French, German, Dutch, English and Italian -- relating to Minsky's wide variety of business operations. Specific findings included documents on his dealings in oil, timber and consumer goods; maps of the Kenya-Sudan border; an inquiry by Minsky concerning Nigerian civil engineering and bridge construction services; an offer from Minsky's Korean representative asking him to ascertain whether Liberian President Charles Taylor would be interested in establishing diplomatic relations with Pyongyang; and a record of a \$30,333.23 payment to Anna Nicole Smith as "a thank you and an apology." Most important, however, police found evidence of several proposed and realized arms deals.

Dec 2008, Phone call in Turkey, Hakan and Celik wire money

US GOVERNMENT TELEPHONE INTERCEPT: [December 3, 2008]

Call placed from a mobile phone (90-242-244-8945) registered in Antalya, Turkey to mobile phone (90-0212-516-90-24) registered in Istanbul, Turkey. Conversation took place in the Kurmanji language on Wednesday, December 3, 2008 at 14:05:00 GMT.

90-242-244-8945: Hakan, we are close to making a deal with- [pause] with our contact. When can you have the money ready?

90-0212-516-90-24: I can have it ready in two weeks. You must give me three days notice, however, if you want to have it in cash. If you want the money wired, I can arrange that within 24 hours. You must not forget, Celik.

90-242-244-8945: Good. I will call you as soon as we know.

Jan 2009, vwparts4salecheep, Jhon meeting jtomski, Arab Sail

payment and shipment

Arab Sail in April

jtomski

alers in London

IGIGENCE REPORT: June 9, 2008 from M15

suspected arms dealers Nicolai Kuryakin and Boonmee  
re registered attendees at the Defence Systems Equipment  
London that began on June 7, 2008.

1

Minsky

Minsky shot in jail cell?

Feb 2009, cocaine bust in Italy, Leonid Minsky, diamonds

Report Date: 2 February 2009 from La Repubblica (Italy)

Rome -- A recent cocaine bust in Italy turned into a surprise of international intrigue. Italian police discovered four prostitutes in a hotel room with a Ukrainian businessman named Leonid Minsky. The police also discovered more than \$35,000 in cash, a half-million dollars in diamonds, and more than 1,500 documents detailing a tangled web of business dealings in oil, diamonds, and gun shipments to Yemen. Two days after Minsky was placed in custody, he was found dead in his cell due to unknown cause. Florence police are being supported in their investigation by UN arms experts.

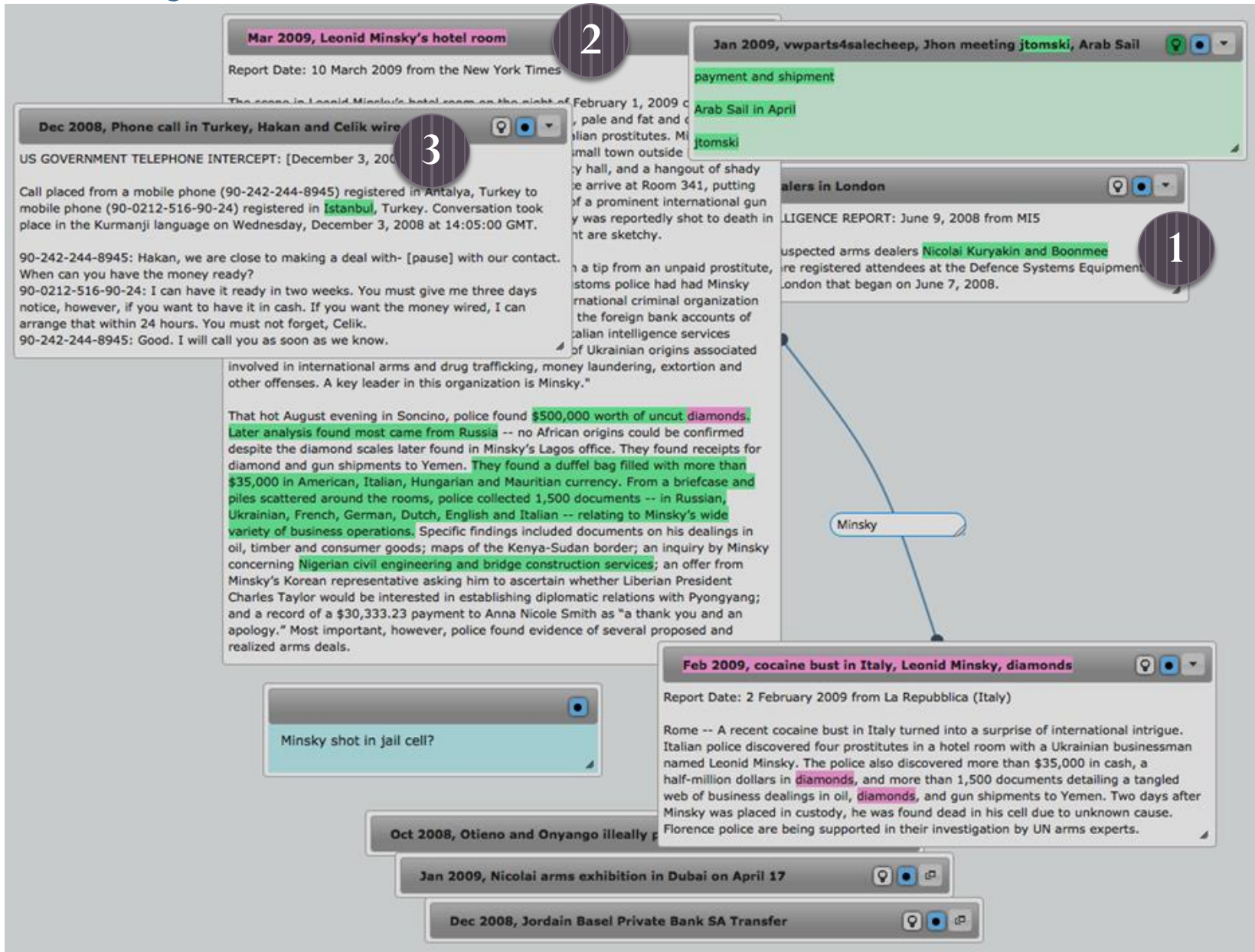
Oct 2008, Otieno and Onyango illegally p

Jan 2009, Nicolai arms exhibition in Dubai on April 17

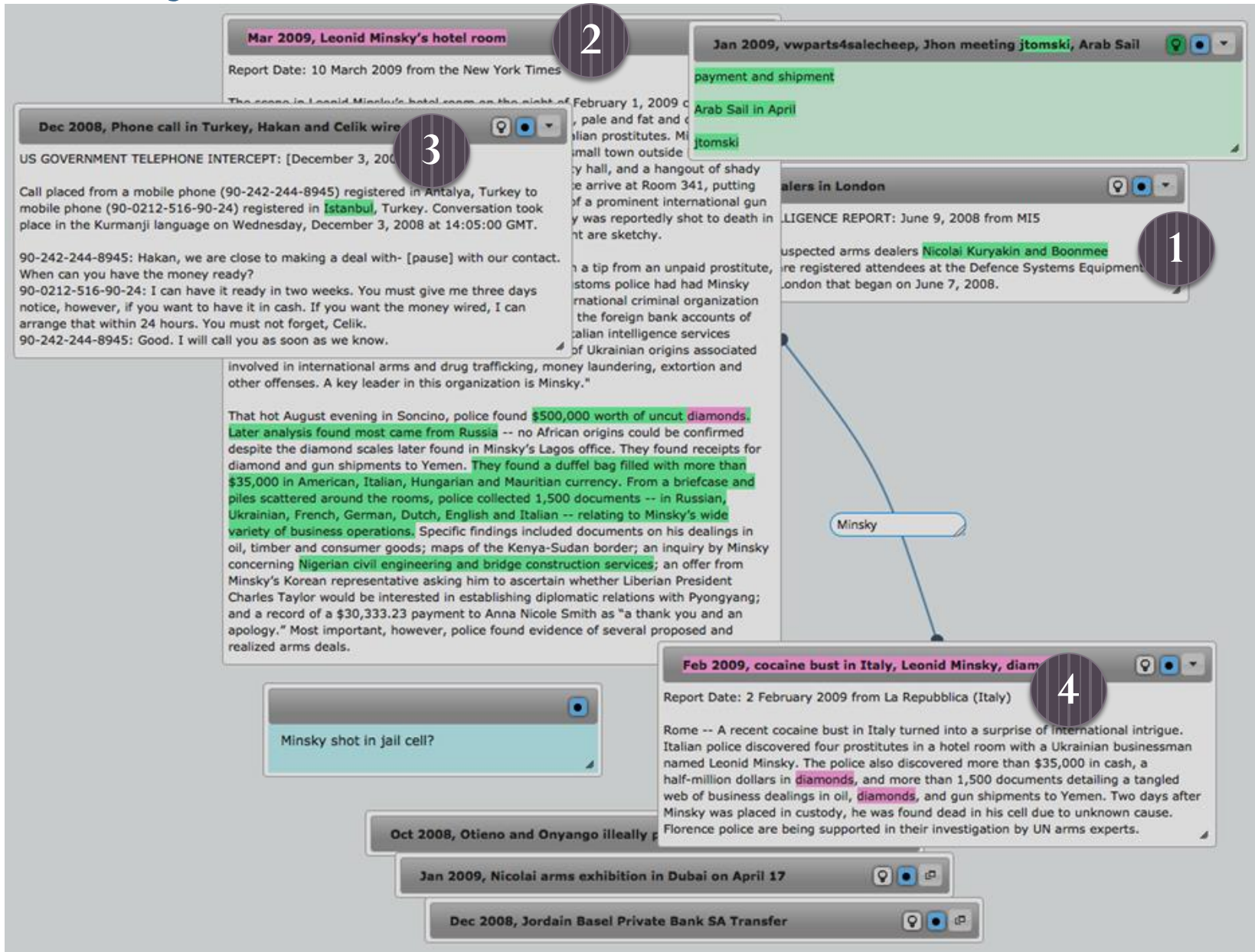
Dec 2008, Jordain Basel Private Bank SA Transfer



# History of Data Interaction



# History of Data Interaction



# Raw Event Logs (example)

0:13:01 – search – “Kenya resources”, 321, 813  
0:13:20 – move document – doc 3204, 110, 323  
0:13:22 – open document – doc 3204, 280, 811  
0:14:01 – move document – doc 440, 331, 500  
0:18:20 – search – “Nicholai” – doc 440, 180, 549  
0:18:29 – open document – doc 1102, 203, 311  
0:19:27 – move document – doc 871, 391, 741  
0:19:29 – open document – doc 12, 410, 683  
0:19:40 – highlight text – “delivery through Tanya” – doc 12, 104, 371  
0:22:57 – open document – doc 3227, 391, 874  
0:23:31 – move document – doc 3227, 341, 349  
0:28:11 – open document – doc 126, 76, 210  
0:31:01 – highlight text – “arrested in hotel lobby following incident” – doc 32, 310  
0:32:45 – move document – doc 32, 354, 891  
0:32:51 – open document – doc 2891, 430, 184  
0:41:09 – move document – doc 100, 432, 9  
0:41:14 – search – “Burj” – doc 1312, 130, 347  
0:32:45 – move document – doc 32, 354, 891  
0:32:51 – open document – doc 2891, 430, 184  
0:41:09 – move document – doc 100, 432, 9  
1:00:45 – move document – doc 32, 354, 891  
1:02:21 – open document – doc 2891, 472, 164  
1:08:34 – move document – doc 132, 242, 931

...

# Segment into chunks of time

0:13:01 – search – “Kenya resources”, 321, 813

0:13:20 – move document – doc 3204, 110, 323

0:13:22 – open document – doc 3204, 280, 811

0:14:01 – move document – doc 440, 331, 500

0:18:20 – search – “Nicholai” – doc 440, 180, 549

---

0:18:29 – open document – doc 1102, 203, 311

0:19:27 – move document – doc 871, 391, 741

0:19:29 – open document – doc 12, 410, 683

---

0:19:40 – highlight text – “delivery through Tanya” – doc 12, 104, 371

0:22:57 – open document – doc 3227, 391, 874

0:23:31 – move document – doc 3227, 341, 349

0:28:11 – open document – doc 126, 76, 210

0:31:01 – highlight text – “arrested in hotel lobby following incident” – doc 32, 310

0:32:45 – move document – doc 32, 354, 891

0:32:51 – open document – doc 2891, 430, 184

---

0:41:09 – move document – doc 100, 432, 9

0:41:14 – search – “Burj” – doc 1312, 130, 347

0:32:45 – move document – doc 32, 354, 891

0:32:51 – open document – doc 2891, 430, 184

0:41:09 – move document – doc 100, 432, 9

1:00:45 – move document – doc 32, 354, 891

1:02:21 – open document – doc 2891, 472, 164

---

1:08:34 – move document – doc 132, 242, 931

...



# Segment into chunks of time\*

T0

0:13:01 – search – “Kenya resources”, 321, 813  
0:13:20 – move document – doc 3204, 110, 323  
0:13:22 – open document – doc 3204, 280, 811  
0:14:01 – move document – doc 440, 331, 500  
0:18:20 – search – “Nicholai” – doc 440, 180, 549

---

T1

0:18:29 – open document – doc 1102, 203, 311  
0:19:27 – move document – doc 871, 391, 741  
0:19:29 – open document – doc 12, 410, 683

---

T2

0:19:40 – highlight text – “delivery through Tanya” – doc 12, 104, 371  
0:22:57 – open document – doc 3227, 391, 874  
0:23:31 – move document – doc 3227, 341, 349  
0:28:11 – open document – doc 126, 76, 210  
0:31:01 – highlight text – “arrested in hotel lobby following incident” – doc 32, 310  
0:32:45 – move document – doc 32, 354, 891  
0:32:51 – open document – doc 2891, 430, 184

---

T3

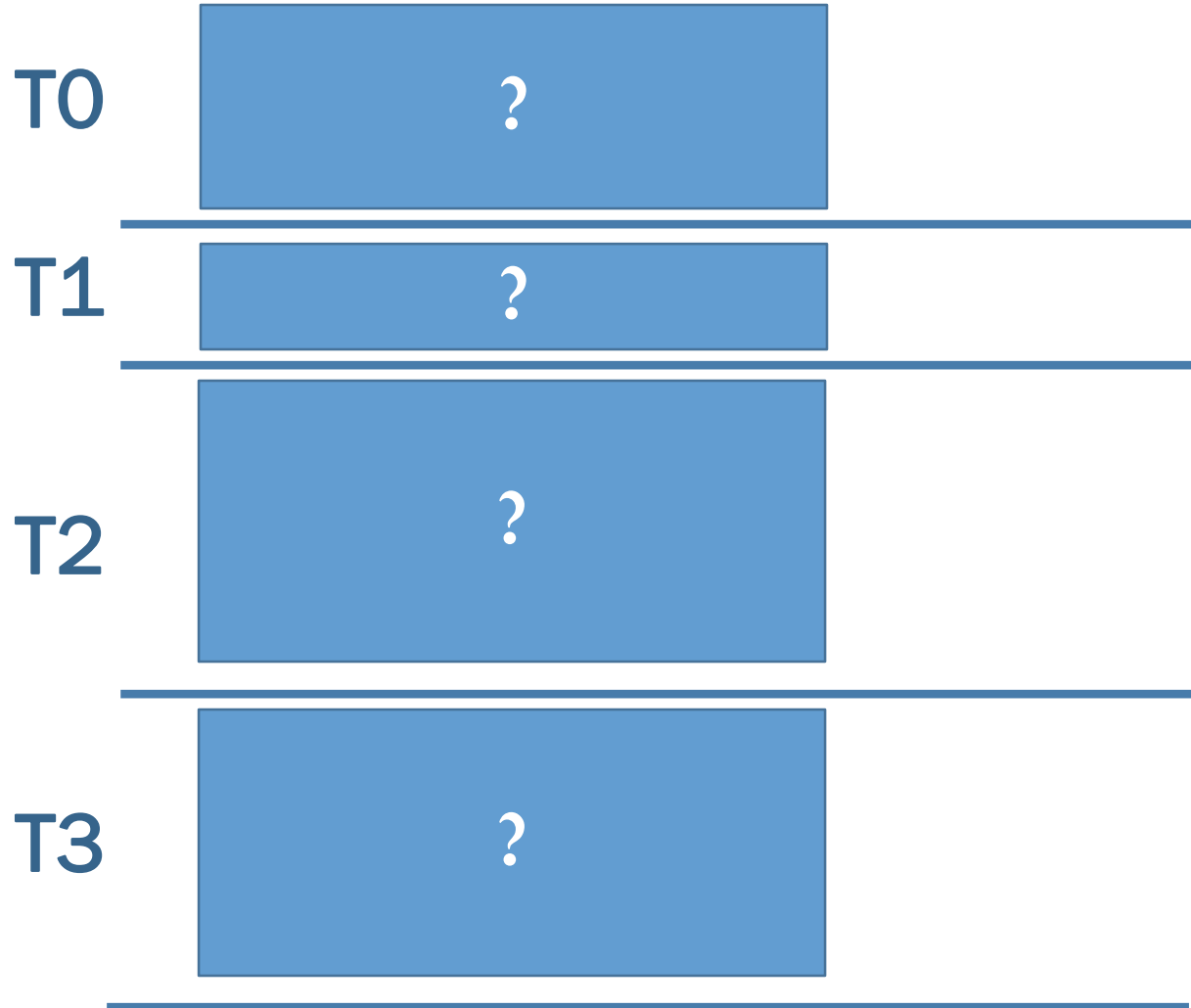
0:41:09 – move document – doc 100, 432, 9  
0:41:14 – search – “Burj” – doc 1312, 130, 347  
0:32:45 – move document – doc 32, 354, 891  
0:32:51 – open document – doc 2891, 430, 184  
0:41:09 – move document – doc 100, 432, 9  
1:00:45 – move document – doc 32, 354, 891  
1:02:21 – open document – doc 2891, 472, 164  
1:08:34 – move document – doc 132, 242, 931

---

...

\*This step is done for you!

# Generate visual summaries for time segments



# Visual Summary Prototyping

Needs design creativity and development for visual summaries

- Data covered in period?
- Interactions used?
- Number of documents/topics reviewed?
- Other behavior?

# Visual Summary Prototyping

Needs design creativity and development for visual summaries

Explored documents related to **arms dealing**, **hotel stays**, and **used auto parts**. Many frequent searches.  
Highlighted: “the deal happens in April”.

