

The world first indictment of bank hacker “Carbanak”

**Prosecutor AnChen Chang
Taipei District Prosecutors' Office**

**10th IAP Asia & Pacific Regional Conference,
Busan, Korea**

Movie or Life?

- Sep. 15, 1995, American Movie “Hackers” released
- 2010, Las Vegas, Black Hat computer security conference, Barnaby Jack demonstrated how to make 2 ATMs dispense cash on stage, like “jackpotting”



Bank Hacker Group “Anunak”

- 2014, Dutch security company **Fox-IT** and Russian security company **Group-IB**, discovered in 2012-2014, a hacker group “**Anunak**” based in Russia and the Ukraine stolen more than \$15 million from Eastern European banks
- **Anunak** members send phishing emails to banking employees that appear to be from the Central Bank of the Russian Federation, but which actually contain malware designed to infect the employees' computers by exploiting recently-patched flaws in Microsoft Office
- They install more malware on the banks' ATMs
- This malware causes the ATMs to muddle up money denominations, meaning a criminal can go to an ATM, request 10100-rouble notes, and receive 105,000-rouble notes instead

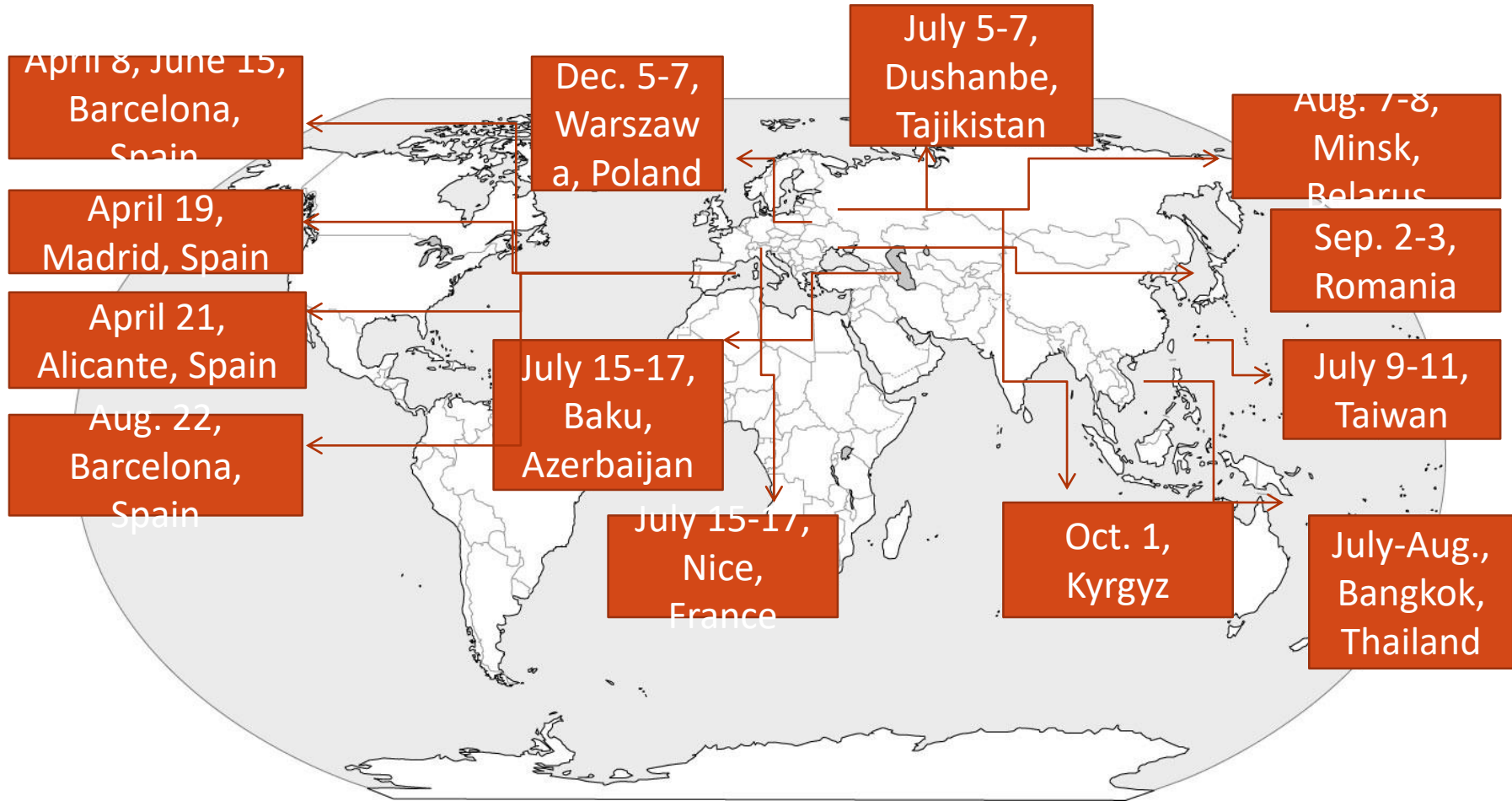
Bank Hacker Group “Carbanak”

- 2014, Kaspersky Lab, under authorization of an Ukraine bank, investigated an incident that an ATM dispensed cashes without anyone around, like “jackpotting”
- 2015, Kaspersky Lab released an official report on the investigation and called the type of attack as “Carbanak”
- Carbanak is a type of hackers’ crime which attacks banks and financial institutes.
- Started in Eastern European
- Crime groups members spam from Chinese, Russians, Ukrainians, Latvians, Romanians, Estonians, Moldovans, to Australians.
- Victim banks over 100, worldwide

Carbanak worldwide attacks

- Sep. 2015, Center for Strategic and International Studies (CSIS) discovered **mutant carbanak malware** targeted banks in **Western Europe** and **America**.
- March 2016, Proofpoint computer security company reported evidences showing that carbanak turned to attack banks in **the Middle East** and the **U.S.**

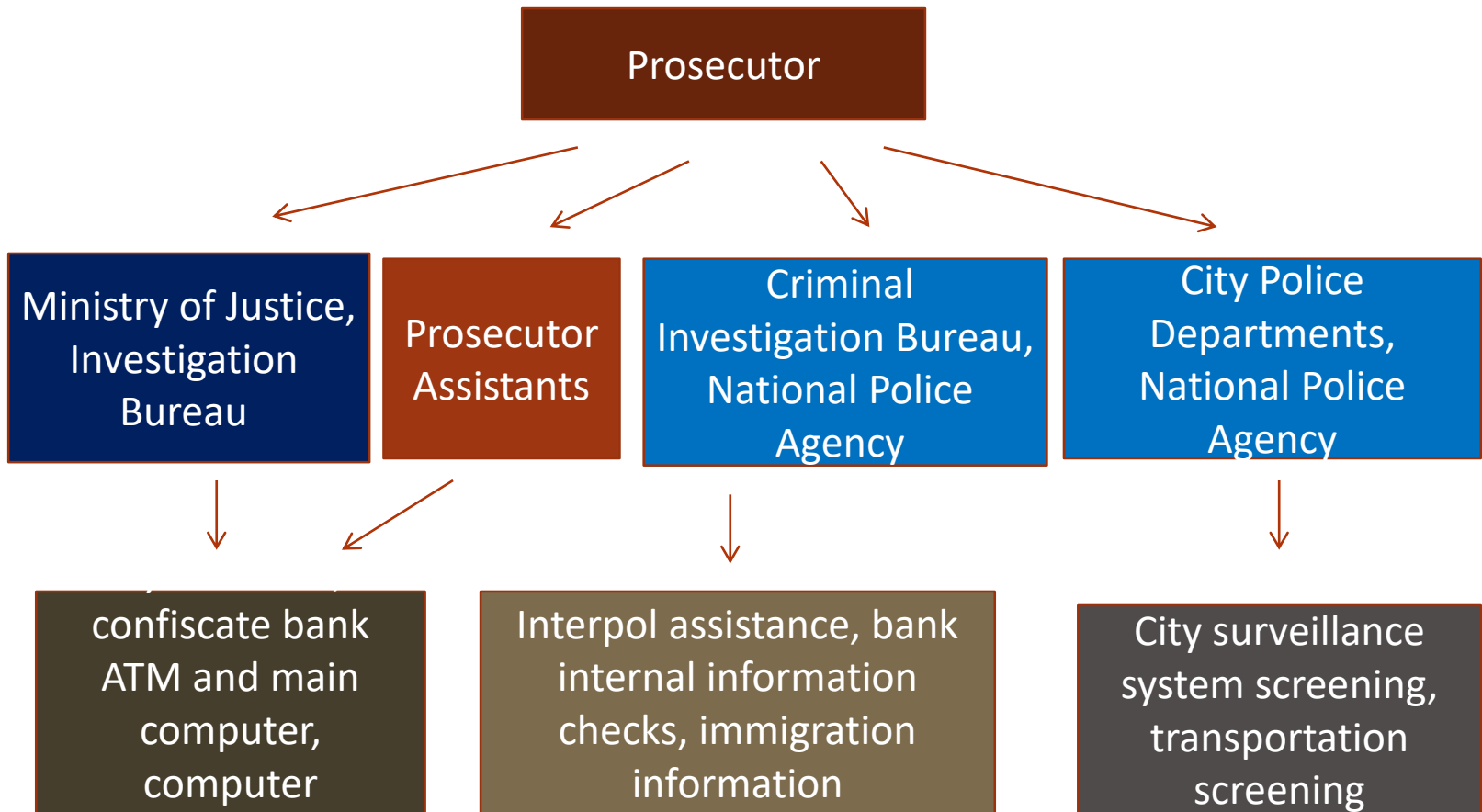
Carbanak worldwide attacks



Carbanak aimed at Taiwan

- 8 pm, July 10, 2016, 2 Russians, Manukian Gaik and Adiiian Kamo, Guting Branch of the First Commercial Bank, Taipei City, get 0.11 million USD, ran into a couple, left 2000 USD cash at ATM
- 2 am, July 11, 2016, 2 Russians, Berezovskiy Sergey, Berkman Vladiair, Nanmen Branch, Taipei City, get 62000 USD, ran into a passer-by Mr. Tsai, Berezovskiy dropped his **credit card** on spot, Mr. Tsai memorized **taxi plate**.
- **22** group members formed **9** groups and flew to Taiwan from Hong Kong, Turkey, Dubai, Philippine, Sydney, and Macau; stayed 1-5 days to withdrew cash from ATMs; **19** of them left for Hong Kong,

Investigation Team



Investigation works

- Over 1000 polices dedicated in reviewing 1500 street monitors, 212 immigration data, 28 websites/facebook of suspects, 23 taxi+15 buses used by suspects—sort out 22 defendants/19 fled overseas, 3 under surveillance in Taiwan
- 53 fingerprints, 45 DNA samples collected from targeted ATM, hotels, and rental cars used by defendants.
- Search Bank headquarter, victim branches, ATM maintenance company
- 2 malwares found, “cngdisp_new.exe”, “cngdisp.exe”
- Hacked ATMs are Type ProCash 1500, produced by

The hacking trace



How 3 Defendants transported stolen cash

- Babii, pick-up, transported 3 luggage to lock in the large lockers of Taipei Main Station on July 12-13, 2016.
- Mihail and Nicolae picked up 3 luggage on July 16, 2016 and checked in Victoria Hotel.
- Andrejs picked up 1 luggage with cask left by other pick-ups in Hyatt Hotel in Taipei and transported it to day-rent apartment.
- Andrejs divided cash into 2 bags and hide them in the bushes near a hiking trail in NeiHu area of Taipei City.
- Andrejs sent out GPS info of these 2 bags to other crime members and headed to YiLan County to hide

The Arrest

- A police accidentally ran into Andrejs in a restaurant of YiLan County and reported to local police station for help.
- Andrejs was arrested on July 17, 2016
- Police monitored Mihail and Nicolae also made arrest on the same day at Victoria Hotel and discovered (100 million USD).





1 bag lost

- Mr. Ko DeLin found the hidden bag and took it home before police came
- After Police released news Ko returned the bag after
- NTD 4,542,200 was found
- Mr. Ko was indicted for em
- A total of NTD 77,485,100 (2.6 million USD) was returned (93.4% of stolen money)



3 Arrested Defendants

分進合擊 赴台盜款

洗錢手 安德魯 (拉脫維亞) 入境 7/11 17:51 從杜拜入境

洗錢手 潘可夫 (羅馬尼亞) 入境 7/16 俄羅斯→韓國→台灣

洗錢手 米海爾 (摩爾多瓦) 入境 7/16 羅馬尼亞→莫斯科→廣州→台灣

車手 貝瑞左夫斯基 柏克曼 (俄羅斯) 7/17 在宜蘭台9線被逮。

7/17 在台北大直維多利亞飯店被逮。

7/17 在台北大直維多利亞飯店被逮。

台灣

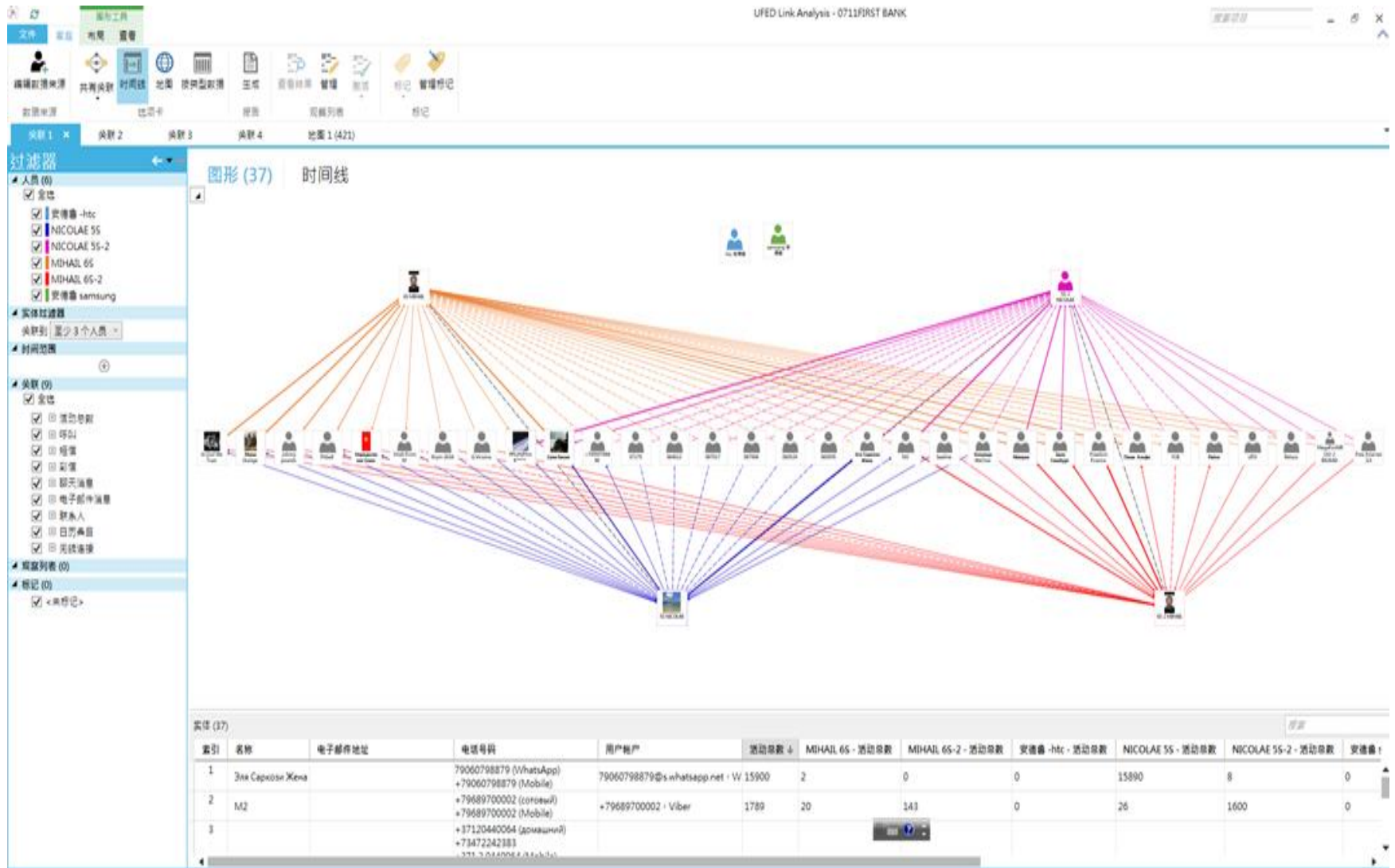
製表：廖炳祺、王宏興
資料來源：警方提供

左起為安德魯、潘可夫及米海爾。記者楊萬雲 / 攝影

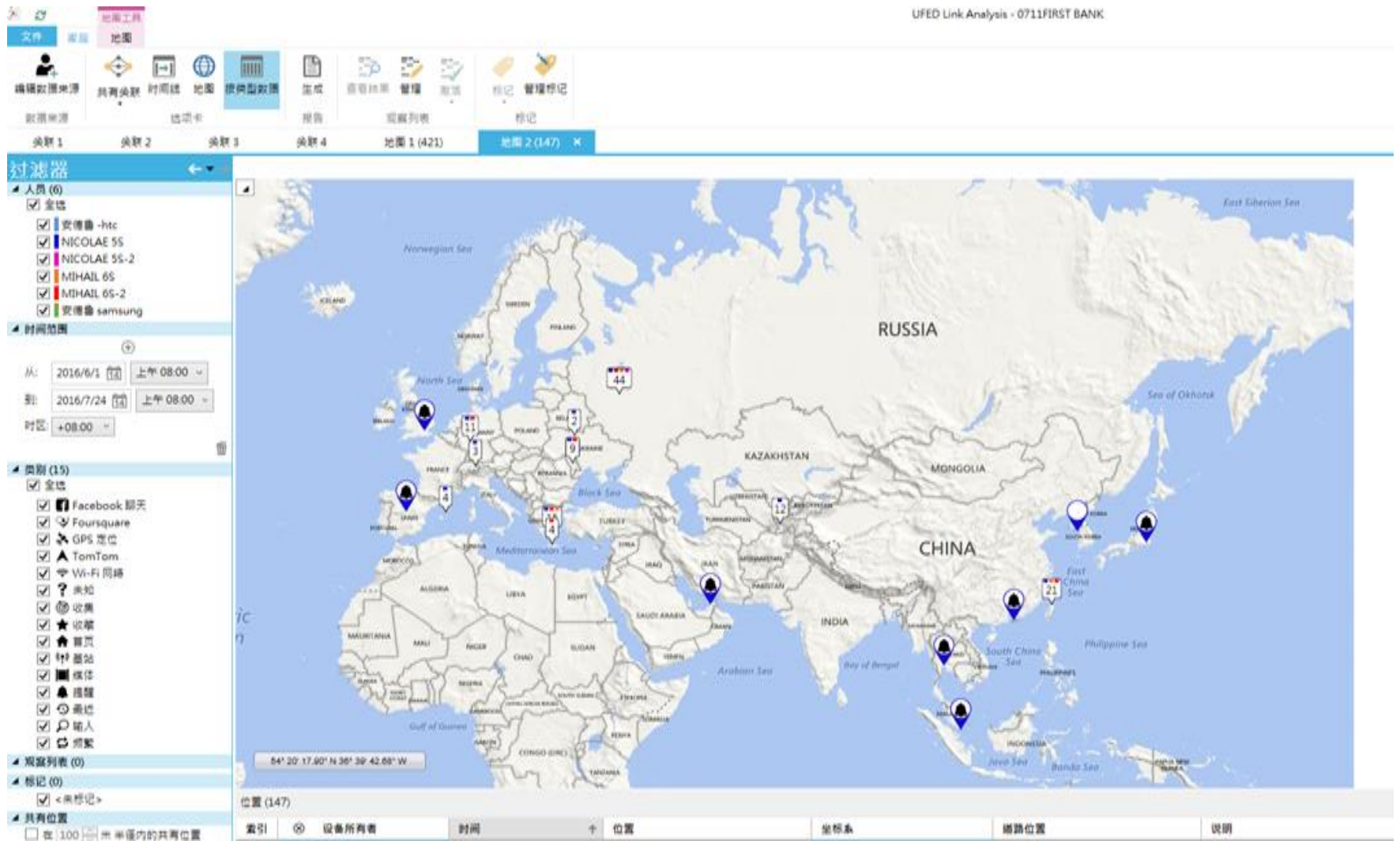
閱報秘書



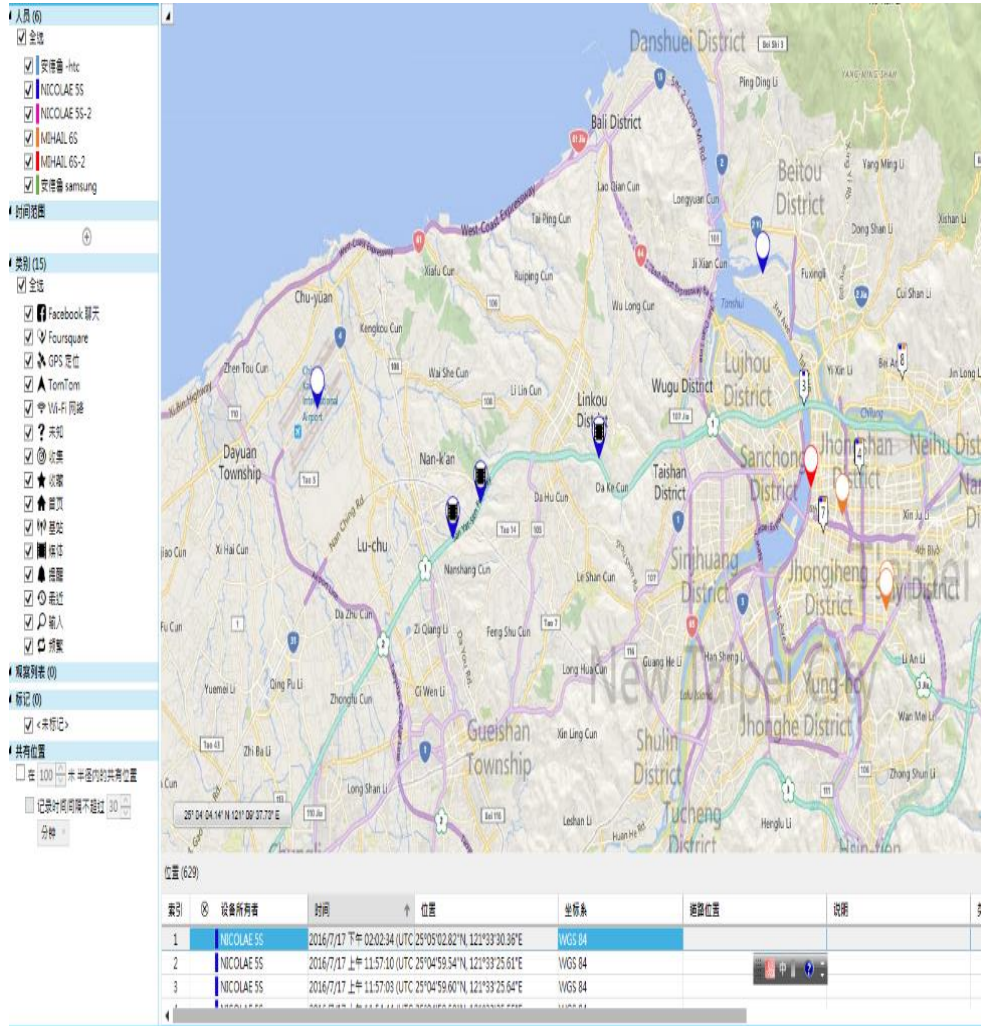
Cross Analysis for Defendant Andrejs's 2 Mobiles



GPS Records from Mihail's and Nicolae's Mobiles(1050601-1050724)




Taiwan GPS Records from Mihail's and Nicolae's Mobiles



Defendant Nicolae's Mobile had cash photos taken in July 7, 2016

Images Go to

Details Events (0)



Name: IMG_4205.JPG
Type: Images
Size (bytes): 1701503
Path: UFO/Media/DCIM/104APPLE/IMG_4205.JPG
Created: 2016/7/7 上午 03:00:32(UTC+0)
Accessed: 2016/7/15 下午 04:44:58(UTC+0)
Modified: 2016/7/7 上午 03:00:32(UTC+0)
Deleted: 2016/7/15 下午 04:44:57(UTC+0)
Extraction: File System
MDS: 1204ce9f1be7225a3e6059201a6684f6
Source file: [IMG_4205.JPG](#)


Metadata

Camera Make: Apple
Camera Model: iPhone 5s
Lat/Lon: 38.567158 / 68.801986
Capture Time: 2016/7/7 上午 08:00:32
Pixel resolution: 3264x2448
Resolution: 72x72 (Unit: Inch)

Map

Images Go to

Details Events (0)



Name: IMG_4204.JPG
Type: Images
Size (bytes): 2086082
Path: UFO/Media/DCIM/104APPLE/IMG_4204.JPG
Created: 2016/7/7 上午 03:00:21(UTC+0)
Accessed: 2016/7/15 下午 04:44:58(UTC+0)
Modified: 2016/7/7 上午 03:00:22(UTC+0)
Deleted: 2016/7/15 下午 04:44:54(UTC+0)
Extraction: File System
MDS: 65e2ee20ab25fef6b257bd011af4da87
Source file: [IMG_4204.JPG](#)


Metadata

Camera Make: Apple
Camera Model: iPhone 5s
Lat/Lon: 38.567158 / 68.801986
Capture Time: 2016/7/7 上午 08:00:21
Pixel resolution: 3264x2448
Resolution: 72x72 (Unit: Inch)

Map

Images Go to

Details Events (0)



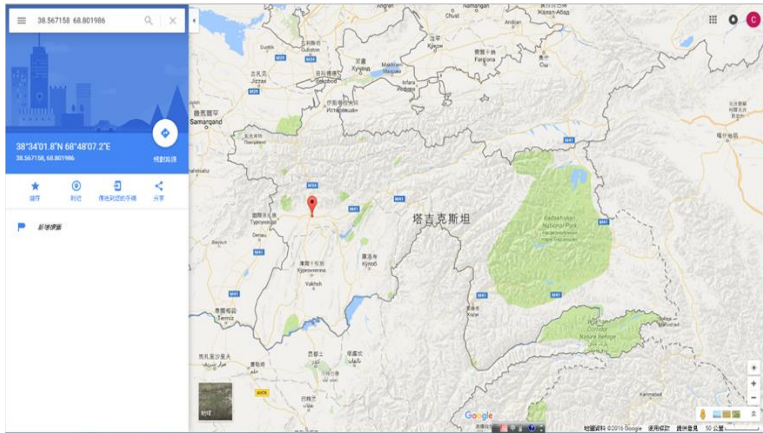
Name: IMG_4203.JPG
Type: Images
Size (bytes): 1751663
Path: UFO/Media/DCIM/104APPLE/IMG_4203.JPG
Created: 2016/7/7 上午 01:48:14(UTC+0)
Accessed: 2016/7/15 下午 04:44:58(UTC+0)
Modified: 2016/7/7 上午 01:48:14(UTC+0)
Deleted: 2016/7/15 下午 04:44:54(UTC+0)
Extraction: File System
MDS: f0f640c5fbee349f89fd59c2b4337563
Source file: [IMG_4203.JPG](#)

Metadata

Camera Make: Apple
Camera Model: iPhone 5s
Lat/Lon: 38.573333 / 68.801925
Capture Time: 2016/7/7 上午 06:48:14
Pixel resolution: 3264x2448
Resolution: 72x72 (Unit: Inch)

Map

Defendant Nicolae's Mobile had photos taken in July 7, 2016, at Tajikistan



Defendant Nicolae's Mobile has payment records for pick-ups

Note

Translate Go to ▾

Title: Аtm 150000P
Creation time: 2014/6/16 下午 02:30:23(UTC+0)
Modification Time: 2016/7/13 下午 12:38:47(UTC+0)
Source: Notes Ha iPhone
Extraction: File System
Source file: Gangster/Applications/group.com.apple.notes/NoteStore.sqlite : 0x7F0FC (Table: ZICLOUDSYNCINGOBJECT, Size: 684032 bytes)
Gangster/Applications/group.com.apple.notes/NoteStore.sqlite/ NoteData_42 : 0xF (Size: 4347 bytes)

Summary

Гриша 400\$

Body HTML Text

Аtm 150000P Гриша 400\$ Рашид 175000P Lai Adrian Андрей толстый 20000 руб Витос 100000 руб Мелентей 500€ Беларус Алишер 1000\$ 18000P Бастрыгин 5000€185000P Коля Саркози 140000P5000P10000P Рустам 700000 руб Кувалда 2500000P Краснодар 90000P95500P+ Варшава 90000P На леху 150000P Француз 60000P Барселона -Франкфурт 4500€ Тайвань 2000€ 30000P 47000P24000P120000P20000P 48115P55000P11000P27844P38854P Стамбул 1500000P 200000P 400\$ 1300€200\$30000P 1300€200\$30000P

Attachment

Map

Google

번역

關閉即時翻譯

英文 白俄羅斯文 中文 偵測語言 ▾

中文(繁體) 白俄羅斯文 英文 ▾ 翻譯

"Аtm 150000P Гриша 400\$ Рашид 175000P Lai Adrian Андрей толстый 20000 руб Витос 100000 руб Мелентей 500€ Беларус Алишер 1000\$ 18000P Бастрыгин 5000€185000P Коля Саркози 140000P5000P10000P Рустам 700000 руб Кувалда 2500000P Краснодар 90000P95500P+ Варшава 90000P На леху 150000P Француз 60000P Барселона -Франкфурт 4500€ Тайвань 2000€ 30000P 47000P24000P120000P20000P 48115P55000P11000P27844P38854P

Стамбул 1500000P 200000P 400\$ 1300€200\$30000P"

А Be ▾

*Аtm 150000P

"提款機150000P Grisha\$400 拉希德175000P 賴 阿德里安 安德魯厚20000盧布 Vitos10萬盧布 Melent'ev500€ 白俄羅斯 阿利舍爾1000\$18000P Bastygin5000€185000P 科爾齊140000P5000P10000P 魯斯塔姆70萬盧布 大錘2500000P 克拉斯諾達爾90000P95500P+ 華沙90000P 在萊赫150000P 法國60000P 巴塞羅那-Frankfurt4500€ 台灣 2000€30000P47000P24000P120000P20000P 1000P27844P38854P

伊斯坦布爾1500000P200000P400\$1.300€\$ 20030000P"

提出修改建議

Google 翻譯企業版： 譯者工具包 網站翻譯工具 全球商機搜尋器

Defendant Mihail's Mobile inquired ATMs information all over the world

海米爾第二支手機

Time	Source	Value	Search Results
2016/4/11 上午 03:10:02(UTC+0)	Google	catalunya caixa atm	加泰羅尼亞儲蓄銀行 ATM
2016/4/11 上午 03:12:00(UTC+0)	Google	spania atm	spania ATM
2016/4/11 上午 03:14:12(UTC+0)	Google	portugal atm	葡萄牙 ATM
2016/4/11 上午 03:21:07(UTC+0)	Google	atm maroco	ATM 品佳昌實業
2016/4/11 上午 03:23:06(UTC+0)	Google	atm france	ATM 法國
2016/4/11 上午 03:25:50(UTC+0)	Google	italy atm	ATM 意大利
2016/4/11 上午 03:28:07(UTC+0)	Google	atm horvatia	ATM horvatia
2016/4/11 上午 03:29:38(UTC+0)	Google	atm norvegia	ATM 挪威
2016/4/11 上午 03:30:32(UTC+0)	Google	atm norway	ATM 挪威
2016/4/11 上午 03:32:43(UTC+0)	Google	atm danemark	ATM danemark
2016/4/11 上午 03:34:42(UTC+0)	Google	atm swizerland	ATM 瑞士

Defendant Mihail's WeChat mentioned Bitcoin, Yacht in Taiwan, Cash in Moscow

2016/7/12 下午 07:14:32(UTC+0)	Google	амекс в тайване	AMEX 台灣
2016/7/12 下午 07:16:10(UTC+0)	Google	амекс в тайване	AMEX 台灣
2016/7/12 下午 12:21:04(UTC+0)	Google	news on taiwan today	今天台灣新聞
2016/7/12 下午 12:41:48(UTC+0)	Google	rent car in taipei	租汽車在台北
2016/7/12 下午 12:59:10(UTC+0)	Google	buy car in taiwan	買汽車在台灣
2016/7/13 上午 08:08:09(UTC+0)	Google	тайбэй стамбул	台北伊斯坦布爾
2016/7/13 上午 08:08:16(UTC+0)	Google	тайбэй стамбул авиа	台北伊斯坦布爾預訂
2016/7/14 下午 05:51:18(UTC+0)	Google	москва тайбэй авиабилеты	莫斯科飛往台北的航班
2016/7/16 上午 06:22:27(UTC+0)	Google	табло прилета тайбэй	台北板到貨

2016/7/12 上午 09:52:29(UTC+0)	Google	русское тур агенство в тайване	在台灣魯斯科旅遊代理
2016/7/12 上午 09:52:31(UTC+0)	Google	русское турагенство в тайване	在台灣的俄羅斯旅行社
2016/7/12 上午 11:03:30(UTC+0)	Google	taiwan news channel	台灣新聞頻道
2016/7/12 下午 01:03:50(UTC+0)	Google	rent house taiwan	租的房子台灣
2016/7/12 下午 02:24:58(UTC+0)	Google	news on taiwan today onlain	台灣今日新聞 onlain
2016/7/12 下午 06:21:55(UTC+0)	Google	можно ли в москве поменять тайванский доллар	是否有可能在莫斯科台灣豆撈改變
2016/7/12 下午 06:21:57(UTC+0)	Google	можно ли в москве обменять тайваньский доллар	無論是在莫斯科兌換新台幣
2016/7/12 下午 06:42:36(UTC+0)	Google	могут ли в Китае проследить купюру по номеру	不管是在中國，以跟蹤號碼的法案
2016/7/12 下午 06:56:09(UTC+0)	Google	могут ли в Китае проследить купюру по номеру где то это используют	不管是在中國，以跟蹤法案它是用於

Defendant Mihail's WeChat Log mentioned Money Laundering

15.	wxid_e1w4eeujcq3r12 Freedom Finance..	Я утром по Гон Конгу хотел сделать. Объем большой и хотел разбавить. 我本來早上想先搞香港的，數目很大，我想把它分成幾份。	WeChat: wxid_e1w4eeujcq3r12..	2016/4/27 下午 07:30:53(UTC+0)..
16.	wxid_c0caavkqsdvp12	Завтра утром?..	WeChat:	2016/4/27 下午
35.	wxid_e1w4eeujcq3r12 Freedom Finance..	Рамин привет. у тебя случайно связей нет в Тайване?.. Ramin, 你在臺灣有沒有管道?..	WeChat: wxid_e1w4eeujcq3r12..	2016/7/10 上午 09:29:12(UTC+0)..
36.	wxid_c0cagykqppvp12 Рома..	Пиши сюда .. 你繼續寫..	WeChat: wxid_e1w4eeujcq3r12..	2016/7/10 上午 09:45:06(UTC+0)..
37.	wxid_e1w4eeujcq3r12 Freedom Finance..	Смотри у меня ребята сейчас в тайбэй в Тайване у них там нала в их валюте почти на 2 лимона \$ в эквиваленте! Ты можешь как то помочь принять его там и что я его в мск получил? 我現在臺灣臺北有人有當地幣的現金，相當於美金2百萬，你可以幫我接收這筆錢，然後讓我在莫斯科領嗎?..	WeChat: wxid_e1w4eeujcq3r12..	2016/7/10 上午 09:54:43(UTC+0)..
38.	wxid_e1w4eeujcq3r12 Freedom Finance..	Это срочный вопрос. Потому что меня подвели люди очень сильно с кем я договаривался .. 這件事很趕，因為我原本談好的那些人給我搞砸了。	WeChat: wxid_e1w4eeujcq3r12..	2016/7/10 上午 09:55:23(UTC+0)..

Messages in Confiscated Mobiles Translated in Chinese

#	From	To	Subject	Body	圖示	Location	Source Application	Timestamp-Date	Timestamp-Time
Instant Messages (15)									
1	+37368288835 Марик			Я там	我到了		iMessage: +79687029995	103/10/19	2014/10/19 下午 11:21:02(UTC+8)
2	+79687029995			Зайди в Тим	那你應該進去 TEAM SPEAK		iMessage: +79687029995	103/10/20	2014/10/20 下午 09:15:25(UTC+8)
3	+37368288835 Марик			Зайди обратно в тим	那你再進去一次		iMessage: +79687029995	103/10/20	2014/10/20 下午 09:26:02(UTC+8)
4	+37368288835 Марик			ruderman oleksandr new york usa money gram от равн ему 750 \$ он мерч подготовит	使用 money gram 寄給他 750美金, 因為這個人會準 備 merch(可能是帳戶或物品)		iMessage: +79687029995	103/10/20	2014/10/20 下午 10:53:27(UTC+8)
5	+79687029995			Через money gram	透過 money gram		iMessage: +79687029995	103/10/20	2014/10/20 下午 10:57:34(UTC+8)
6	+37368288835 Марик			Да	是的		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:32:01(UTC+8)
7	+79687029995			Понял	了解		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:35:22(UTC+8)
8	+79687029995			Я завтра иду в одно тур агенство по поводу виз ы в Америку! Сказали помогут 100%	我明天要去一個旅行社處理美國簽證, 那裏的人 說百分之百可以幫付		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:53:28(UTC+8)
9	+37368288835 Марик			Возьми меня с собой	那你帶我一起去		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:54:00(UTC+8)
10	+37368288835 Марик)))	(笑臉)		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:54:06(UTC+8)
11	+79687029995			Я посмотрю завтра что то должен заполнить и н а конец недели в посольство	我看看要處理什麼文件, 禮拜一要去辦事處		iMessage: +79687029995	103/10/20	2014/10/20 下午 11:55:16(UTC+8)
12	+37368288835 Марик			В багаж бери если что))))))	把我放心裡面		iMessage: +79687029995	103/10/21	2014/10/21 上午 12:05:58(UTC+8)
13	+79687029995			👉👉👉👉			iMessage: +79687029995	103/10/21	2014/10/21 上午 12:06:17(UTC+8)
14	+37368288835 Марик			Зайди в тим спик	進去 TEAM SPEAK		iMessage: +79687029995	103/10/21	2014/10/21 上午 03:32:55(UTC+8)
15	+37368288835 Марик			+37259681029 мой вайбер	viber的帳號		iMessage: +79687029995	103/10/22	2014/10/22 下午 04:36:16(UTC+8)

Passport photos from confiscated mobiles



2BAC5B56-C383-4748-8E63-4FB956415A9F_original.jpg



FirstImageOriginal.jpeg



IMG_0584.PNG



IMG_0597.JPG



IMG_0598.JPG



IMG_0603.JPG



IMG_0604.JPG



IMG_2843.PNG



IMG_2844.PNG



IMG_2901.JPG



IMG_3209.JPG



IMG_4093.JPG



IMG_4574.JPG



IMG_4594.JPG



IMG_4595.JPG



IMG_4596.JPG



IMG_6009.PNG



IMG_6341.PNG



IMG_6357.PNG



IMG_6735.PNG



IMG_7034 (2).JPG



IMG_7034.JPG



IMG_7034_1.JPG



IMG_7054.JPG



IMG_7324.JPG



IMG_7341.JPG



IMG_7377.PNG



IMG_7896.JPG



IMG_8502.JPG



IMG_8523.JPG



IMG_8595.JPG



IMG_8596.JPG



IMG_8723.JPG



IMG_9363.JPG



IMG_9364.JPG



IMG_9431.JPG



IMG_9878.JPG



Паспорта.rar_embedded_1 (2).jpg



Паспорта.rar_embedded_1.jpg



Паспорта.rar_embedded_1_1.jpg



Паспорта.rar_embedded_2 (2).jpg



Паспорта.rar_embedded_2.jpg



Паспорта.rar_embedded_2_1.jpg



Паспорта.rar_embedded_3 (2).jpg



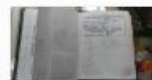
Паспорта.rar_embedded_3.jpg



Паспорта.rar_embedded_3_1.jpg

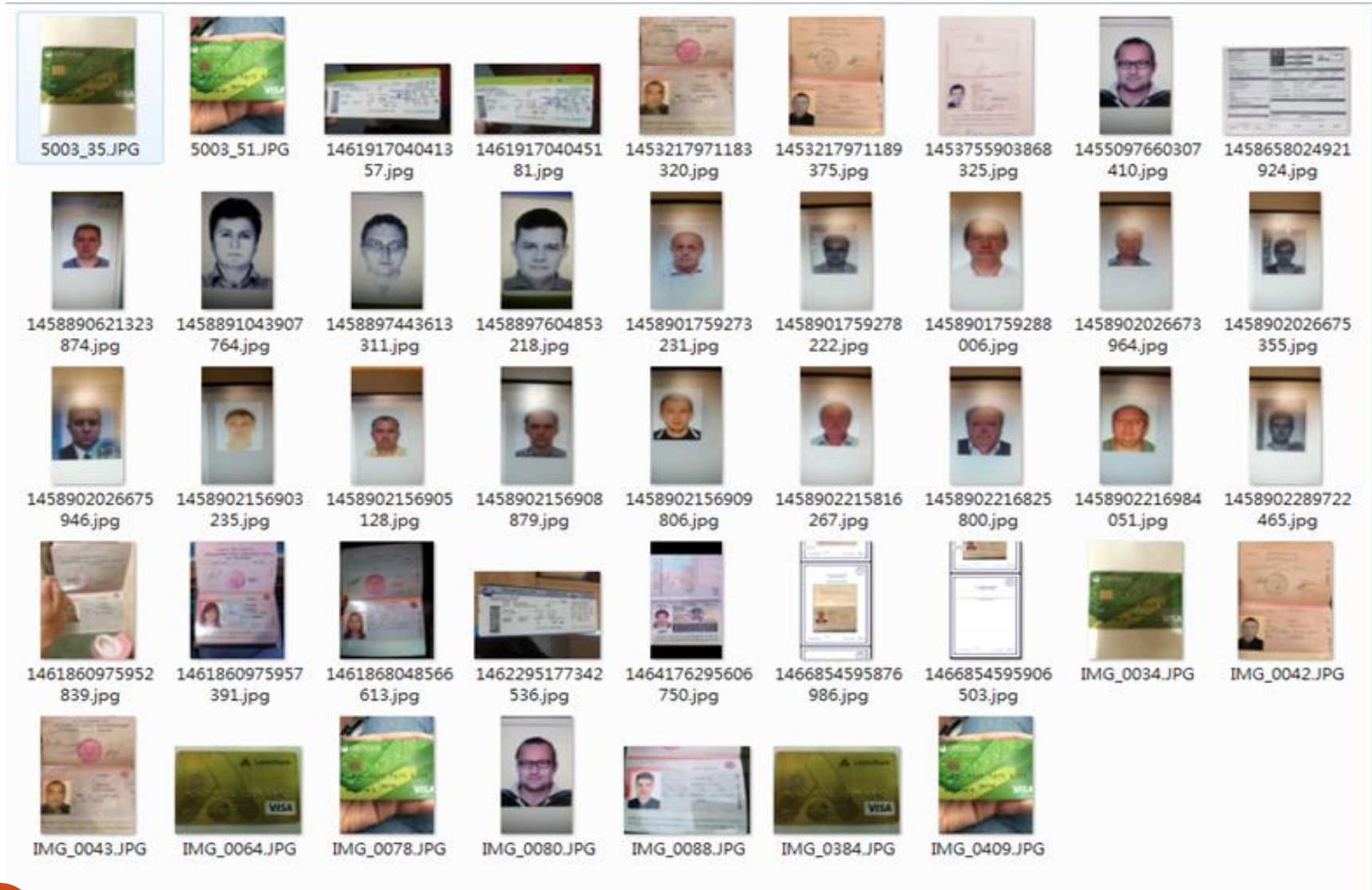


Паспорта.rar_embedded_4.jpg



Паспорта.rar_embedded_4_1.jpg

Passport photos from confiscated mobiles



Cash Photos found in confiscated mobiles



Indictement

- Sep. 9, 2016, prosecutor Lee YenLin indicted 3 defendants for **12 accounts** of charges violating the criminal law:
 - **§339-2** fraud ATM
 - **§358** invading others' computer
 - **§359** changing others' computer record without reason
 - **§360** interfere others computer with a computer program without reason
 - **§362** make computer programs to obstruct computer uses
- Issued want warrants for other 19 defendants
- 3 defendants detained in Taipei Detention Center

District Court Judgement

- 3 defendants denied as members of the Carbanak fraud group and argued that they only received instructions to come to Taiwan but had no idea with any illegality.
- Judging from their mobiles records and the fact that 3 defendants actually actively involved in money laundering before they came to Taiwan, Court overruled their arguments.
- Taipei District Court sentenced each defendants for **5 years incarceration** plus NTD **100,000 fines** (i.e. 3300 USD) on January 25, 2017.
- 3 judge tribunal disagreed with prosecutor's 12 accounts charges but decided only for 1 account of charges.

- The court judgment also mentioned they felt sorry that the maximum sentencing of the charges was only

World First Carbanak Case established

- Thailand, Romania, Belarus, Moldova, and Europol contacted for mutual legal assistance.
- Romania and Europol sent polices to Taiwan to interrogate Mihail and Andrejs for more information
- Babii was later arrested by Belarus police and Romania is negotiating for extradition
- Penkov Nicolae may involve in case in Moldova and under investigation
- More Mutual Legal Assistance is coming.

Future task of computer crimes

- Symantec: (Internet Security Threat Report, 2016) 430 million malwares newly discovered in 2015; 429 million ID leaked (at 15% report rate); encrypted ransom ware increased
- Kaspersky Lab: April, 2016, hackers attack industrial control system to steal gasoline and coal
- Kaspersky Lab: June, 2016, discovered xDedic black market, selling infected server licenses at the price of 6 US dollars; 70624 serves in 174 countries, by 416 dealers
- Kaspersky Lab: malware “Darkhotel”, hackers attack hotels’ wifi to steal business secrets

Fighting Against Enemy Like Shadow

