Forensics Investigation Report

Case 112

Prepared for

Head of Forensic Department

By

Usman Basharat

Table of Contents

1. INTRODUCTION

1.1 Nature of incident

Suspected Terrorism

Daniel McGowan was arrested at Gatwick airport trying to travel with a false passport. One of the customs officials recognised his face from the documentary “If a Tree Falls”. He was travelling with only carry-on luggage and the only digital evidence found on him was the USB that had been seized and placed into evidence.

Any photos of animals found in the investigation represent child pornography and should be considered as evidence. The exception to this is the photos found in the “\MyBlog” and “\Phone Backup” directories.

1.1.1 Location

Gatwick Airport

2. VICTIMS

2.1 Victim details

Hans Murschenhofer lives in Schenefeld, Germany at aged 41. He has habits of being a heavy drinker, drug abuse and child pornography. Even though he has his own illegal activities, Jack Ascroft is blackmailing Hans Murschenhofer in order to of their own interest. This suggests that Hans has no choice, but to follow orders from Hans. Tony is a victim due to the nature of him being arrested. Daniel blackmailed his family if Tony spills to the police what the investigation is going on. However, there are legal implications of the suspects being wrongly accused. Therefore, there will be carried out a full investigation in a professional matter of preventing anything of hiding or destroying any evidence.

3. LOCATION OF EVIDENCE

3.1 Evidence description

3.1.1 Device Type

A USB device, which belonged to Mr Daniel McGowan, has been seized by the Police during an arrest at Gatwick airport.

3.1.2 System, Network, Server Descriptions

3.1.2.1 System 1

N/A

3.2 Seizure details

Daniel McGowan has been arrested at Gatwick airport for trying to travel with a false passport. When searched he was found to have a USB device on him. He had no other technology, not even a mobile phone. The USB was seized at the time of the arrest and placed into evidence.

3.3 Handling Details (Chain of Custody)

3/12/2016 USB device belonging to Daniel McGowan was seized at Gatwick Airport

4/12/2016 USB device was imaged and given to the Forensics Dept. for further investigation. There are two parts to the image – part 1 and part 2. Both are required for analysis.

9/02/2017 Data downloaded and files explored and viewed by me (Encase)

10/02/2017 13:00 Data received is explored and investigated by using various tools (Encase)

17/02/2017 13:00 Data received is explored and investigated by using various tools (Encase)

24/02/2017 12:00 Data received is explored and investigated by using various tools (Encase)

3/03/2017 13:00 Data received is explored and investigated by using various tools (Encase)

6/03/2017 18:00 Data received is explored and investigated by using various tools (Autopsy)

7/03/2017 14:00 Data received is explored and investigated by using various tools (Encase)

9/03/2017 12:00 Data received is explored and investigated by using various tools (Encase)

10/03/2017 12:00 Warrant was received to have access to the Facebook account.

11/03/2017 13:00 Data explored and investigated by using various tools (Autopsy)

17/03/2017 2:30 Data received is explored and investigated by using various tools (Encase)

18/03/2017 12:30 Data received is explored and investigated by using various tools

3.4 Location of Evidence

The original USB has been placed in the secure locker, No 1625.
A copy of the evidence has been passed to the Forensic Department for analysis.

4. DEFINITIONS

4.1 Definitions

Acquisition of Digital Evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collection of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.

Data Objects: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

Digital Evidence: Information of probative value stored or transmitted in digital form. Physical Items: Items on which data objects or information may be stored and/or through which data objects are transferred.

Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.

Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Hash – is a value that is a string of characters that transforms into a shorter value that represents its original value.

Steganography – is a practice of concealing messages or information within other documents.

MD5 – is an algorithm that is used to verify data by producing a hash function of 128 bit has value. Every hash function is unique even when one value is changed, the whole 128 bit value changes.

SHA-1 (Secure Hash Algorithm 1) – is a hash function that is usually expressed as a 160 bit hex number. It is also used to identify any data corruption by checking if the files have been tempered with its original.

Bit – is a short binary digit that represents the smallest unit in the computer system by usually being characters of 0 and 1.

Base 64 – is a combination of binary-to-text that encoding schemes represents binary data in ASCII.

Binary – is used to represent any type of text that usually represents 0 and 1 and this can be used to store data.

Font – is a type of different styles the way the text is being displayed

ASCII – stands for American Standard Code for Information Interchange that allows computers to understand the difference between ‘a’ and ‘A’. In ASCII, there are different types of characters such as the alphabet, numbers, and any characters on the keyboard. These are usually represented as a 7-bit binary number.

Hexadecimal – is a way of expressing binary numbers in computers by using Base 16 as it usually contains 0 to 9 as numbers and from 10 to 15 it is represented as the first five letters of the alphabet. For example 10 would be A.

JPEG – is a type of image file format that allows images to be viewed for compressed image files.

PNG – stands for Portable Network Graphics that is a file format that uses compresses image files that can be viewed.

DOC – is an abbreviation of document that is a file extension for most commonly Microsoft Word.

ZIP – is a file format that that is compressed full of files. Typically, a zip file contains more than one file that is compressed to save memory space.

File Extension – is short characters that usually represents the filename and file type. For example, image1.jpg, the file extension is "jpg" and it is represents as an image.

Compressed – it reduced the number of files it contains by the reduction of the data. Compressed files is usually used to transport data easily.

Encryption – is an unauthorised person cannot read a translation of data that allows. This is most effective way of securing data when transporting it to another person. In order to read the data, a password is required, which is typically known to unlock the data and read what is inside.

Decryption – is a way of process of encrypting data and uncovering the unreadable data into text so that it can be read.

4.2 Tools

HashMyFiles – A tool that is used for files to calculate its file signature such as MD5 and SHA1 hashes in the system.

Password Recovery ToolKit (PRTK) – A tool used to identify and recover any passwords of a file from various different type of file types.

Encase V6 – Data recovery tool that is used to analyse data and information of the files that is used within the evidence that is added.

Encase V7 – Data recovery tool that is used to analyse data and information of the files that is used within the evidence that is added. An upgraded version of Encase V6.

Forensics ToolKit (FTK) – A similar tool kit to Encase used for data recovery by analysing, filtering through thoroughly of the data added. Any deleted information can be recovered.

Autopsy 4.3.0 – A similar kit to FTK that has similar that analyses information of the files that is used within the evidence that is added.

Notepad – A similar tool to Microsoft Word that allows is typically used to note text down on a plain document.

HexEditor – is a computer program that allows editing, viewing and extracting content of a file. The data of the file is shown in hexadecimal and translated to text for users to read.

Windows Photo Viewer – A tool that is used that allows any image to be viewed.

Windows Media Player – A multimedia player that allows any video, music and any other familiar Media Player format to be played on this platform.

VLC Media Player – A cross-platform media that is used to view rewind any videos on the same extension.

OpenPuff – is a tool that lets the user hide and unhide data in files such as images, audios, and videos.

Adobe Acrobat Reader – is used to view, create and save PDF files.

Google (Hex to Text Converter, ASCII to text Converter, (Encode and Decode) Base64 to Text Converter and Base4 to Image Converter) – Google is a search engine which is used to convert evidence from its chosen format from the list shown above.

Microsoft Office including Word, Excel, PowerPoint – A Microsoft Office product that is used to create and store documents for various types of reasons.

5. PRESERVATION OF EVIDENCE

5.1 Validation of Original Evidence

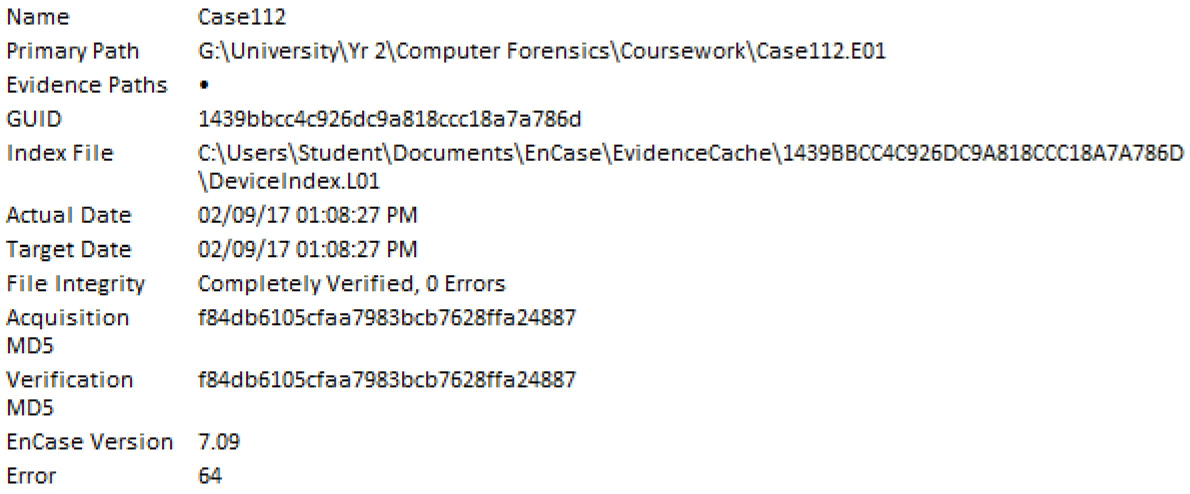
5.1.1 Procedures

Before the investigation, I confirmed that these files were not tampered with when the investigation is being carried out, and then checking whether or not they match up by the original copy of the evidence. The software 'HashMyFiles' software was used to validate the original evidence.

5.1.2 Result

Case112.E01
MD5: 54914ef638249ecb9c166e5680755bcb
SHA1: 27ca3f6c22f031059c6b6c11362dd93d963875a0

Case112.E02
MD5: 7f7cb2781f99d31caab8a39f28a26ff2
SHA1: ab67f2ae12cc3a985046ea28a5f1cf7845016e7d



Name	Case112
Primary Path	G:\University\Yr 2\Computer Forensics\Coursework\Case112.E01
Evidence Paths	•
GUID	1439bbcc4c926dc9a818ccc18a7a786d
Index File	C:\Users\Student\Documents\EnCase\EvidenceCache\1439BBCC4C926DC9A818CCC18A7A786D \DeviceIndex.L01
Actual Date	02/09/17 01:08:27 PM
Target Date	02/09/17 01:08:27 PM
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	f84db6105cfaa7983bcb7628ffa24887
Verification MD5	f84db6105cfaa7983bcb7628ffa24887
EnCase Version	7.09
Error	64

Figure 1 shows in Encase v7 no errors have been found in the Case112.E01

5.1.3 Validation

Hash My Files software left me with the results above. This shows that the data given to me has not been tampered in any way. Each evidence file has a unique hash set. By using an external source to compare the hashes, this shows that the results have been successful. The results above show that the initial hash matches with the results above. The hashing can be complete at any point of the investigation to make sure that the files are correct. Referring to Figure 1, I used Encase v7 to verify that there have been no errors on this evidence file as evident.

5.2 Imaging

5.2.1 Procedures

The evidence from the USB of the suspect that was taken at Gatwick Airport was hashed in order to verify that the given files were not tampered with when the investigation of this case is carried out. The initial hashing of the evidence given was analysed by Investigator Diane Gan who verified the evidence files and the exact copy was given to me.

5.2.2 Result

Case112.E01
MD5: 54914ef638249ecb9c166e5680755bcb
SHA1: 27ca3f6c22f031059c6b6c11362dd93d963875a0

Case112.E02
MD5: 7f7cb2781f99d31caab8a39f28a26ff2
SHA1: ab67f2ae12cc3a985046ea28a5f1cf7845016e7d

5.2.3 Validation

The results present shows that the above results have been successfully hashed. This shows that the files have been maintained during the whole course of the investigation and the hashing of the evidence given the above result can be done at any point.

6. ANALYSIS STEPS

6.1 Procedures

In order to view all the files, I used Encase v6 to view them and export those files displayed in Encase to take certain procedures as shown below.

6.1.1 Emails

I need your services.eml

For this email, it was located under "*MyBlog*" under "*Blog*", this email was viewed on Encase v6, and I highlighted the text to view the text hidden in this email. I viewed the text by changing its format and I saw this the email communicating from Miko (Hacker) to Daniel. This evidence is as a screenshot within Appendix under 9.1.1.

Katie to Wang.eml

For this email, it was encrypted. Therefore, I had to use a numerous of tools to find the password. I used OpenPuff to find a hidden message within XKCD364 folder within Comms. I found an image that had the hidden text file for a public key and private key. In addition, I unlocked this using the password on the image. Once this was unlocked, I used Kleopatra software to decrypt the image. There is a password for decrypting the email, which I used "Passphrase" as written next to it and it decrypted the message to Katie to Wang. It came with a attached image. Therefore, I did used Base64 converter to image and found the attached image. This evidence is under Appendix 9.1.14 and 9.1.15.

6.1.2 Messages

Timeisprecious.ps1

This was saved as a ps1 extension. I saw on Encase v6 that there was a hidden message on their which is the following, "*#hey Daniel, thought you might find this useful, have fun. Miko.*" This is a message sent from Miko (Hacker) as a message. Underneath this, it was a hex message that was converted using Google by searching Hex to Text Converter. I converted this message leading me to a code. However, this did not lead me to anywhere so I continued my search.

The Lord of the Rings

On Encase, I did a search for the password. I found a message that was found hidden in the "*The Lord of the Rings". This said, "Oh. It is quite simple. If you are a friend, you speak the password and the door will open".* I found this hidden message within the text in that file. However, this message says something; however, it did not lead me anywhere.

Wp-trackbackb6ad.php

This was found on under MyBlog and I found this file. This was saved as a php. On Encase, it showed that there was a hidden message by an unknown source. It stated, "*I really need an ID for this to work."* This shows that there has been a conversation between two unknown people; however, I did not manage to get anywhere. Therefore, I continued my search for this.

6.1.3 Tools

OpenPuff – 1.jpg 2.jpg 3.jpg 4.jpg

For these images, I used this to get a hidden message between these images of *WhatsAppDanielKatie.txt*. I used OpenPuff to find the hidden message. I realised that there was an order for these messages with a password. Therefore, I recognised that 2.jpg had a station name called *Potsdamer Platz*. I put in this as a password with a number of combinations of the images. A first few tries have been unsuccessful, however I tried 4.jpg 3.jpg 1.jpg 2.jpg and it worked to reveal the WhatsAppDanielKatie.txt appeared as evidence in Appendix under 9.1.7.

Facebook

As explained below, as soon as I found out about SE Report. There were details about his Facebook Username and Password. I knew that I could not access these until I have a warrant to access someone's account. Therefore, I waited until 10th Friday 2017 to access his Facebook account. Once I did this, I realised there was a conversation between Hans and Jack. I found these child pornography pictures within the chat as evidence. The chat can be found below in Appendix under 9.1.8.

Password Recovery ToolKit (PRTK) – GIFs

For PTRK, I used GIFs to be put into the software PRTK. Once these were ran through PRTK, I found passwords for all of the GIFs in the evidence file. Some of them were running and some of them were not. However, I did find 11 passwords hidden in these GIFs. Unfortunately, it did not lead me anywhere. Therefore, I continued my search.

6.1.4 Files

Fwd. It is almost time for your stay at the Grand Elysée Hotel Hamburg.jpg

I first decided to investigate "Fwd. It's almost time for your stay at the Grand Elysée Hotel Hamburg.jpg" file within "Temp" folder. I saw on Encase v6 that it was saved as a jpg, but when I tried to double click it, it said, "The File extension has A HTML file signature, but "jpg" extension". After this, I realised that the file extension was an HMTL file extension. I changed this to HTML and found a forwarded email from LateRoom.com to Daniel's email. In the email, it had booking details of where he is staying, what, how, arrival and departure dates to Hamburg. A screenshot of the booking details for Daniel is proof in Appendix under 9.1.2.

XKCD Link

I later decided to investigate the folder names that was in the folder "*LOLZ*". There is an image file *aHR0cHM6Ly9nb28uZ2wvRDBwWmJa.jpg*. I realised that this was base64, so I converted this by searching up Base 64 converter on Google. I decoded this to a link to https://goo.gl/D0pZbZ and this directed me to https://xkcd.com/936/ . This link indicated to me about password strength. I later realised that I have seen *XKCD* name within the "Comms" folder. There is a folder there named XKCD364. I saw there was a match in the previous link that I found. This link https://xkcd.com/364/ led me to another image, which indicated of responsible behaviour. However, both of these links did not lead me to anywhere. Therefore, I continued my search.

ZIPs

NoAttachments.doc

By using Encase, you can check if any folder has any extended folders compressed within them i.e. ZIPs. By clicking view file structure, it would either show you if the file is a zip or not in Encase. I did this for NoAttachments.doc in WIP. I found out that this is a zip. I extracted the folders and later I investigated further into these folders. I saw a file called *OleObject1.bin*, which I browsed, however there was an error in this. I wanted to see what the code behind in is this. Therefore, I changed the extension of this to a text file. I later discovered that Daniel and Katie were having a conversation about a Chinese deal in Manchester. I later discovered that there was an image in this text email. Therefore, I opened up FTK, viewed the exact email on FTK, and found the attached broken image. This can be found in Appendix under 9.1.4 and 9.1.5.

11-220 Records.xlsx

I later found another zip file in Encase stored in "MyBlog" called 11-220 Records.xlsx. I did the same technique with the NoAttachment.doc as for this file 11-220 Records.xlsx. For this file, I found numerous of images located inside "xl > media"; I found images and one of the unbroken image Katie was talking about to Daniel (Main Suspect) in the text file. This is displayed in Appendix under 9.1.6.

SE Report

For SE Report, I found a file called, "*SE Report.7z*" under "*MyBlog*". I found this to be a zip file that has a password on this. Therefore, I read the previous emails that I have found. This linked to Daniel and Miko (Hacker) having a conversation about getting information on Hans. Miko, as stated in the email, likes to find discover passwords, which was found the last thing he did on his Facebook. Therefore, as this zip file, I did a quick search on Facebook and found Hans Murschenhofer. The last thing he did was he went shopping as stated in German, "Einkaufen". I typed this in and it was successful as the email stated. I found within the zip file a SE Report.jpg extracted. I then opened up HexEdit and changed the first few bits to "25 50 44 46" and changed the file extension to pdf and found a report that Miko attached. This evidence is found in Appendix under 9.1.3.

List of Folder Names

For the List of Names, I decoded the File Names using Base 64 converter located in *Temp*. I decoded these messages to "*Never gonna give you up, Never gonna let you down, Never gonna run around and desert"* I thought this would lead to a password, but it did not get my anywhere. Therefore, I continued my search.

NKHOD Travel

For this, I found that this was password protected. Therefore, I tried numerous of times through PTRK, but it crashed. Therefore, I went to search for the password. I went *to **Fwd. It is almost time for your stay at the Grand Elysée Hotel Hamburg.jpg*** and opened this up in text. I pressed CTRL + F to search for a flight. I saw beside it, it was a password that I tried, "Zxs*9uess8&^dUuG*HMHb@3". I typed this in and it worked. Inside this PDF, it opened up a booking for Jack's booking to Hamburg. This can be found in Appendix under 9.1.9.

7. RESULTS

7.1 Pertinent Hidden Message Summaries

7.1.1 Document 1 Summary – ***Boron Trifuoride*** <PDF Document> *false extension*

This document was hidden within "*MyBlog>SupportDaniel.org>IMAGES". This hidden document was saved as a Boron Trifuoride.GIF. However, when coming across it, I investigated further to find that the extension had been wrong. I changed this to a pdf and this revealed as a Hazardous Substance Fact Sheet for Boron Trifuoride.

7.1.2 Document 2 Summary – **NoAttachment.doc<**Word Document> *hidden message*

This linked within the hidden link that was found within ***NoAttachments.zip > Word.*** A file called Document.xml. I changed this to Document.html. I found a link below that was converted using Base 64 converter in Google. Below link, it was also found in NoAttachments.doc as the same link when the whole document was highlighted red. aHR0cHM6Ly93d3cuYWxpYmFiYS5jb20vcHJvZHVjdC1kZXRhaWwvQm9yb24tVHJpZmx1b3JpZGUtVHJpZXRoYW5vbGFtaW5lLUNvbXBsZXgtaW4tQ2hpbmFfNDkxNzMxOTE5Lmh0bWw/c3BtPWEyNzAwLjc3MjQ4MzguMC4wLm82dzBWbCZzPXA= this was converted to https://www.alibaba.com/product-detail/Boron-Trifluoride-Triethanolamine-Complex-in-China_491731919.html?spm=a2700.7724838.0.0.o6w0Vl&s=p

This linked above revealed Boron Trifluoride Triethanolamine Complex in China linking it together with the Hazardous email.

7.2 Pertinent Images Summary

7.2.1 Image 1 Summary– ***1.jpg 2.jpg 3.jpg 4.jpg*** <Text Message> *DanielKatieWhatsapp.txt – Hidden Message*

This file was found hidden, using OpenPuff, in "*LOLZ>Katie*". The images located in this folder was used in order of 4312. 2.jpg had a station inside on it. Therefore, I used it for the password, I got a conversation between Daniel and Katie about Tony being arrested, and they need another animal lover for the Chinese deal to be in contact. By analysing this using OpenPuff, I was able to get the hidden message within these hidden images.

7.2.2 Image 2 Summary - 20151114_121418.jpg <ASC File> **Katie katie_cutegirl@outlook.com (0x46D012D7) pub-sec.asc** *Hidden file within Images*

This file was found hidden, using OpenPuff, in "*Comms> XKCD364". This image located in this folder was used to find the public and private key towards decrypting the Daniel to Wang.eml. I used Ludwigsplatz. However, I changed the bit selection options to *JPEG>Maximum.* This revealed the public and private key towards unlocking the email.

7.2.3 Image 3 Summary - 20160606_145154.JPG, 20160606_152929.JPG, 20160606_153214.JPG, vedett-dm2wheels7201.JPG. <ASC File> *Hidden Image*

I used OpenPuff for to unlock an image attached to three images and one video located in "*WIP>NACH". This image confirmed the purchase of the hazardous gas under Appendix in 9.1.13. These entire three link in with Boron Trifuoride found having a connection in all three places with the gas as stated above about the same gas.

7.2.4 Image 4 Summary - ***Fwd. It is almost time for your stay at the Grand Elysée Hotel Hamburg.jpg*** (JPG File) *false extension, hidden files*

For this file, the file extension had a false extension. It was initially saved as a JPG. However, when coming across it, I investigated further to find that the extension had been wrong. I changed it to html and from this; it was Daniel's booking receipt to Hamburg.

7.2.5 Image 5 Summary – 7 Images found in 11-220 Records.zip <JPG File> *Hidden Images*

I found 11-220 Records saved as an Excel spreadsheet with numerous of names. I used an Encase Tool to reveal that it was in fact a zip file. I changed this to a zip file and found numerous of images within this zip file located in "*XL> Media". There are about nine images within these files and some of them have connections with others.

7.2.6 Image 6 Summary – Child Pornography Images represented as animals <JPG File>

I was given access by given a warrant from Diane on 10th March to have access to Hans Murschenhofer's Facebook. I found these child pornography images on Han's chat with Jack. Jack sent them to Hans as a blackmail in order to meet him in Rathaus, Hamburg.

[CONTINUED IN APPENDIX 11.1]

8. CONCLUSIONS

8.1 Executive Summary

The summary highlights this case is various evidence that is found, but all of the evidence that I found it, all links in all together. Evidence shown that it began with a conversation between Daniel and Katie discussing their old Chinese contacts in Manchester with a broken image attached. The image attached is found fixed version to have a list of Heroin that Katie is later going to discuss with the Chinese dealer. We later found this out that Tony was arrested when cops found two keys on him. Daniel and Katie both discussed that they needed a replacement. Therefore, Daniel did a background check on Hans Murschenhofer later on and paid the Miko (Hacker) to find out his details.

Later on, it was confirmed that Jack Ascroft booked a ticket to Hamburg between 22/11/2016 to 28/11/2016. He flew and in Hamburg, later on, he contacted Hans Murschenhofer by blackmailing him with the set of images that was found by the Hacker in the email of "I need your services.eml". This clearly indicates that Daniel and Jack have clear exchange of conversation between them and wants Hans to do the job that Tony used to do, because of Han's clean record; he can travel freely. He used those images to blackmail Hans and meet him at a point in Rathaus, Hamburg at 17:00.

Later on, Katie discussed and secured the deal with the old Chinese contacts in Manchester by discussing a rate pf 7%. Old Chinese contacts agree with the 5 kilos of Heroin, at $113.7 a gram that is $568,500 in total.
Katie also stated that they would send half a kilo at a time. This matches in with the Case bio that provides that Katie does drug dealing.

Another evidence that links in with the WhatsApp conversation is Daniel stated that they only have one shot at G20. A quick Google search gave us evidence that G20 is a meeting possibly of 19 countries with their prime minister to have some sort of discussion. Later on, we found a hidden link that gave us a link of Boron Trifuoride that costs US $210-280 Kilograms. We got a payment confirmation of this too. All of these link in with the Boron Trifuoride PDF document and the link. All three link in together. However, due to insufficient evidence found, I could not find a connection between G20, Boron Trifuoride, and the Floor Plan.

9. APPENDIX

9.1 Evidence

9.1.1 Evidence gained from I need your service.eml [I need your service.eml]

daniel.mcgowan10@outlook.com
29/11/2016 21:12
To: m1k0_hakker@outlook.com

Re: I need your service
Excellent! I enjoyed the little challenge, I think I will use it for some of my stuff. Just what we were looking for, I'll pay the standard fee as well as a nice bonus for you. Check your bitwallet. Let me know if you have any issues.
Been good working with you, will get in touch if we have other jobs required.
Daniel

From: m1k0_hakker@outlook.com
Sent: 12 November 2016 21:07
To: daniel.mcgowan10@outlook.com
Subject: Re: I need your service

Found some great stuff on him, got some real dirt there, you shouldn't have any trouble with this. I've attached a report, I've attached a report, you can find the images from this link https://goo.gl/XvQjDg.

By the way, I have a tradition of adding a little challenge to opening the report. You'll have to do some research of your own to discover the password for the zip file, it's the last thing Hans did on his facebook page :) You might want to change some things on the file inside too...

Miko

From: daniel.mcgowan10@outlook.com
Sent: 06 November 2016 21:05
To: m1k0_hakker@outlook.com
Subject: Re: I need your service

Looks good, go for it.

From: m1k0_hakker@outlook.com
Sent: 03 November 2016 21:04
To: daniel.mcgowan10@outlook.com
Subject: Re: I need your service

I've found some initial information on him in preparation for a social engineering attack.He's registered on the archery site archerydirect.de, if you give the go ahead I'll purchase the domain archerydirects.de and send him a password reset email from there.

Please confirm you want me to continue.

Miko

From: daniel.mcgowan10@outlook.com
Sent: 03 November 2016 21:01
To: m1k0_hakker@outlook.com
Subject: Re: I need your service

Unfortunately we don’t have much information on him, just his name and the city he lives in.

Hans Murschenhofer, and he’s based in Hamburg.
Again, try to find some dirt on him that we can use as blackmail material.
Good luck.

Daniel

From: m1k0_hakker@outlook.com
Sent: 03 November 2016 20:59
To: daniel.mcgowan10@outlook.com
Subject: Re: I need your service

Hi Daniel,

That’s what I specialise in. Please provide me whatever information you have on him, keep in mind that the more you give me the faster I’ll find stuff on him, the cheaper it’ll be for you :)

Miko

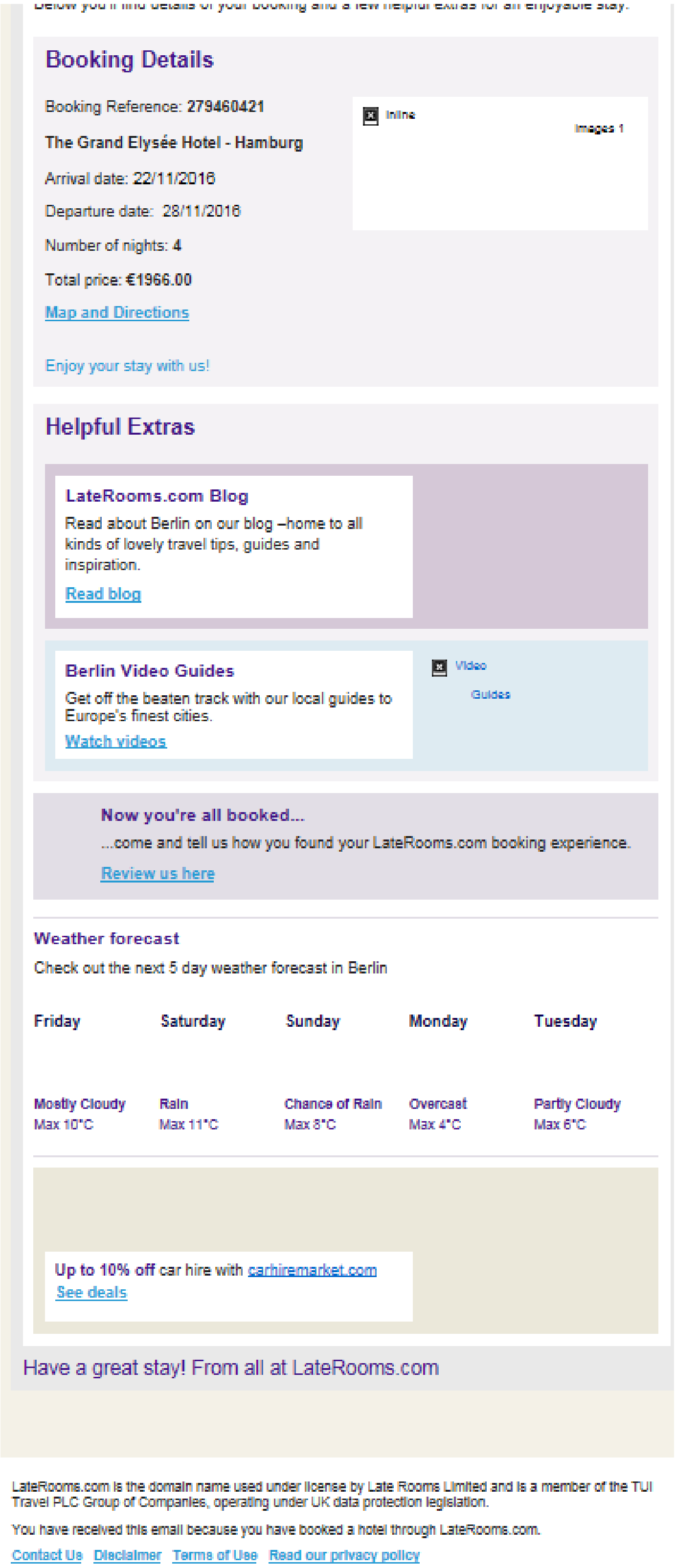
From: daniel.mcgowan10@outlook.com
Sent: 03 November 2016 20:54
To: m1k0_hakker@outlook.com
Subject: I need your service

Miko,

I’d like to hire you to find information on someone. We are hoping to find something that will give us some leverage over him. We don’t care how it’s done. Does this sound like something you can do?

Daniel

9.1.2 Evidence gained from Fwd. It's almost time for your stay at the Grand Elysée Hotel Hamburg.jpg [HTML]



Below you'll find details of your booking and a few helpful extras for an enjoyable stay.

Booking Details

Booking Reference: **279460421**

The Grand Elysée Hotel - Hamburg

Arrival date: 22/11/2016

Departure date: 28/11/2016

Number of nights: **4**

Total price: **€1966.00**

Map and Directions

Enjoy your stay with us!

Helpful Extras

LateRooms.com Blog

Read about Berlin on our blog –home to all kinds of lovely travel tips, guides and inspiration.

Read blog

Berlin Video Guides

Get off the beaten track with our local guides to Europe's finest cities.

Watch videos

Now you're all booked...

...come and tell us how you found your LateRooms.com booking experience.

Review us here

Weather forecast

Check out the next 5 day weather forecast in Berlin

Friday	Saturday	Sunday	Monday	Tuesday
Mostly Cloudy Max 10°C	Rain Max 11°C	Chance of Rain Max 8°C	Overcast Max 4°C	Partly Cloudy Max 6°C

Up to 10% off car hire with carhiremarket.com
See deals

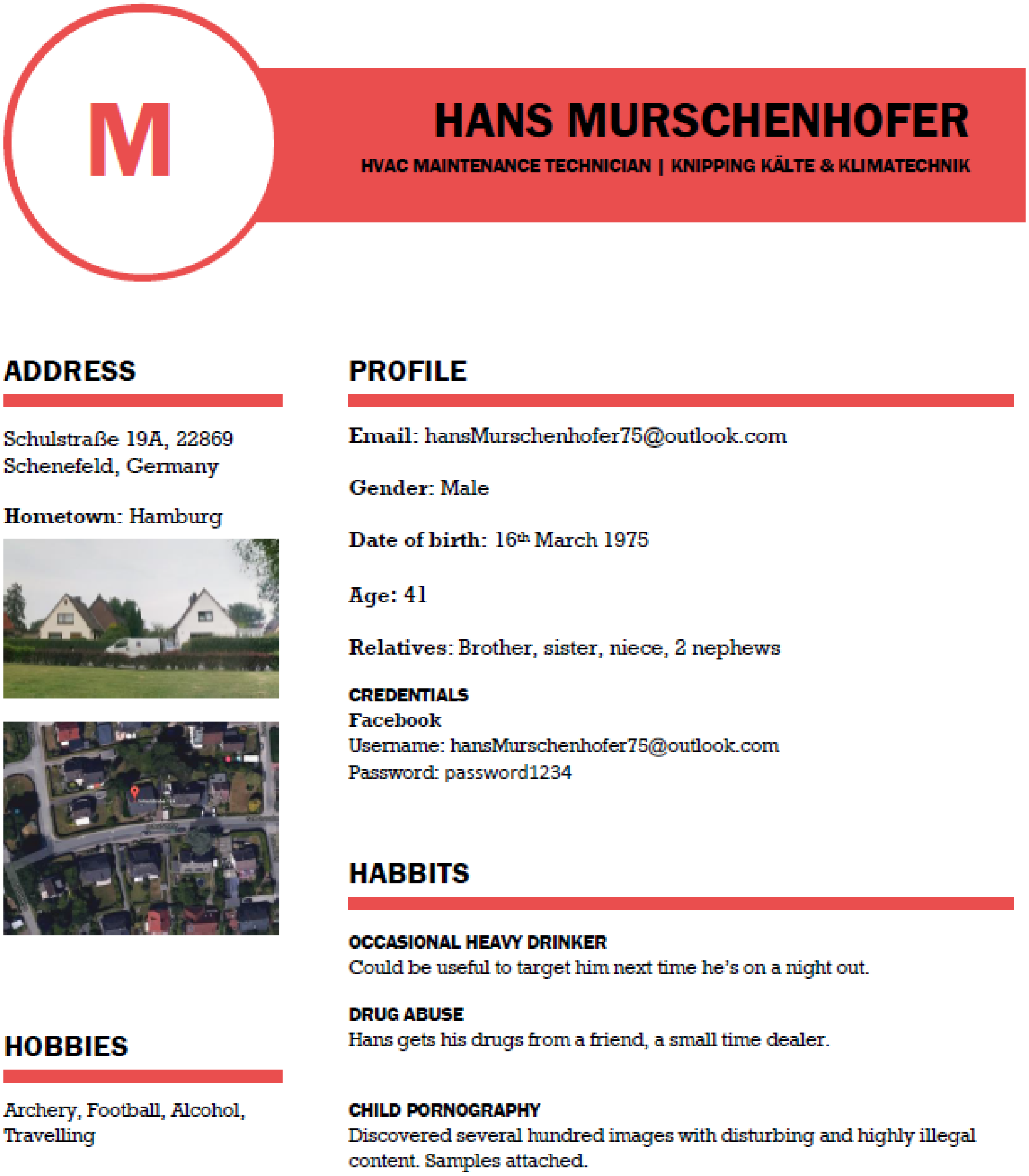
Have a great stay! From all at LateRooms.com

LateRooms.com is the domain name used under license by Late Rooms Limited and is a member of the TUI Travel PLC Group of Companies, operating under UK data protection legislation.

You have received this email because you have booked a hotel through LateRooms.com.

Contact Us   Disclaimer   Terms of Use   Read our privacy policy

9.1.3 Evidence gained from SE Report.7z [SE Report.pdf]



M

HANS MURSCHENHOFER

HVAC MAINTENANCE TECHNICIAN | KNIPPING KÄLTE & KLIMATECHNIK

ADDRESS

Schulstraße 19A, 22869
Schenefeld, Germany

Hometown: Hamburg

PROFILE

Email: hansMurschenhofer75@outlook.com

Gender: Male

Date of birth: 16th March 1975

Age: 41

Relatives: Brother, sister, niece, 2 nephews

CREDENTIALS
Facebook
Username: hansMurschenhofer75@outlook.com
Password: password1234

HABBITS

OCCASIONAL HEAVY DRINKER
Could be useful to target him next time he's on a night out.

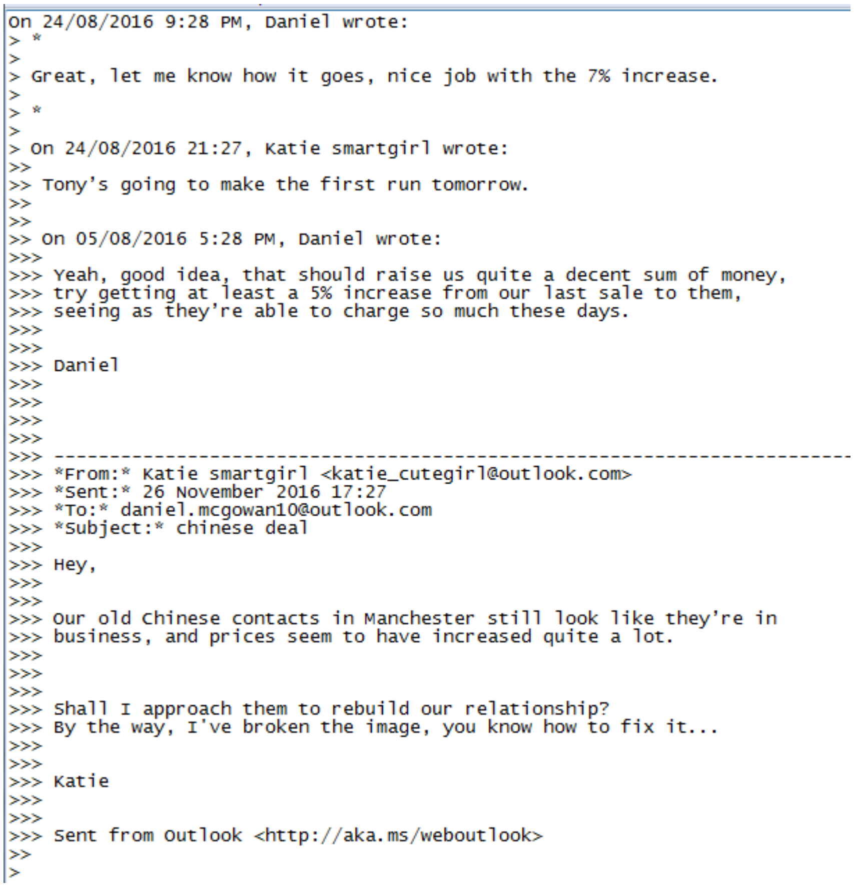
DRUG ABUSE
Hans gets his drugs from a friend, a small time dealer.

CHILD PORNOGRAPHY
Discovered several hundred images with disturbing and highly illegal content. Samples attached.

HOBBIES

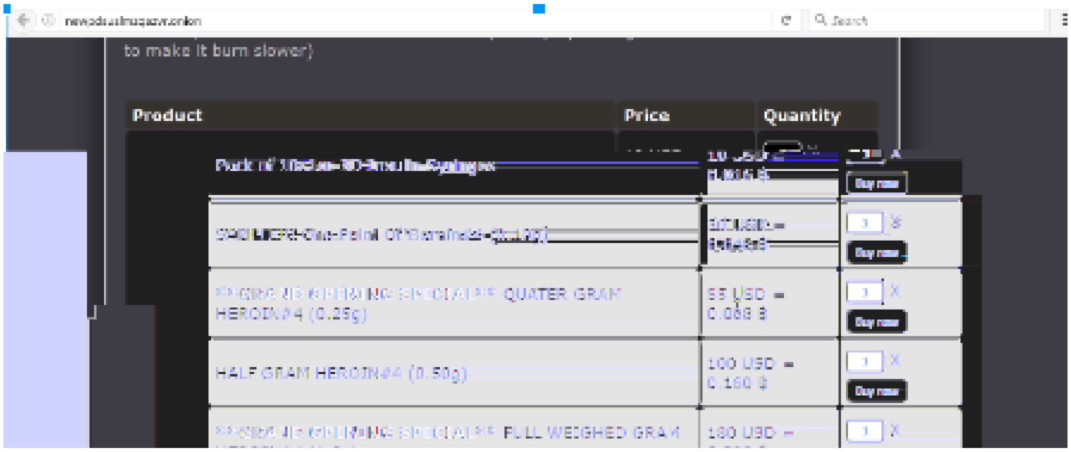
Archery, Football, Alcohol, Travelling

9.1.4 Evidence gained from NoAttachments.docx [NoAttachments.zip – Word – Embeddings]



```
On 24/08/2016 9:28 PM, Daniel wrote:
> *
>
> Great, let me know how it goes, nice job with the 7% increase.
>
> *
>
> On 24/08/2016 21:27, Katie smartgirl wrote:
>>
>> Tony's going to make the first run tomorrow.
>>
>>
>> On 05/08/2016 5:28 PM, Daniel wrote:
>>>
>>> Yeah, good idea, that should raise us quite a decent sum of money,
>>> try getting at least a 5% increase from our last sale to them,
>>> seeing as they're able to charge so much these days.
>>>
>>>
>>> Daniel
>>>
>>>
>>>
>>>
>>> ------------------------------------------------------------------------
>>> *From:* Katie smartgirl <katie_cutegirl@outlook.com>
>>> *Sent:* 26 November 2016 17:27
>>> *To:* daniel.mcgowan10@outlook.com
>>> *Subject:* chinese deal
>>>
>>> Hey,
>>>
>>>
>>> Our old Chinese contacts in Manchester still look like they're in
>>> business, and prices seem to have increased quite a lot.
>>>
>>>
>>>
>>> Shall I approach them to rebuild our relationship?
>>> By the way, I've broken the image, you know how to fix it...
>>>
>>>
>>> Katie
>>>
>>>
>>> Sent from Outlook <http://aka.ms/weboutlook>
>>
>
```

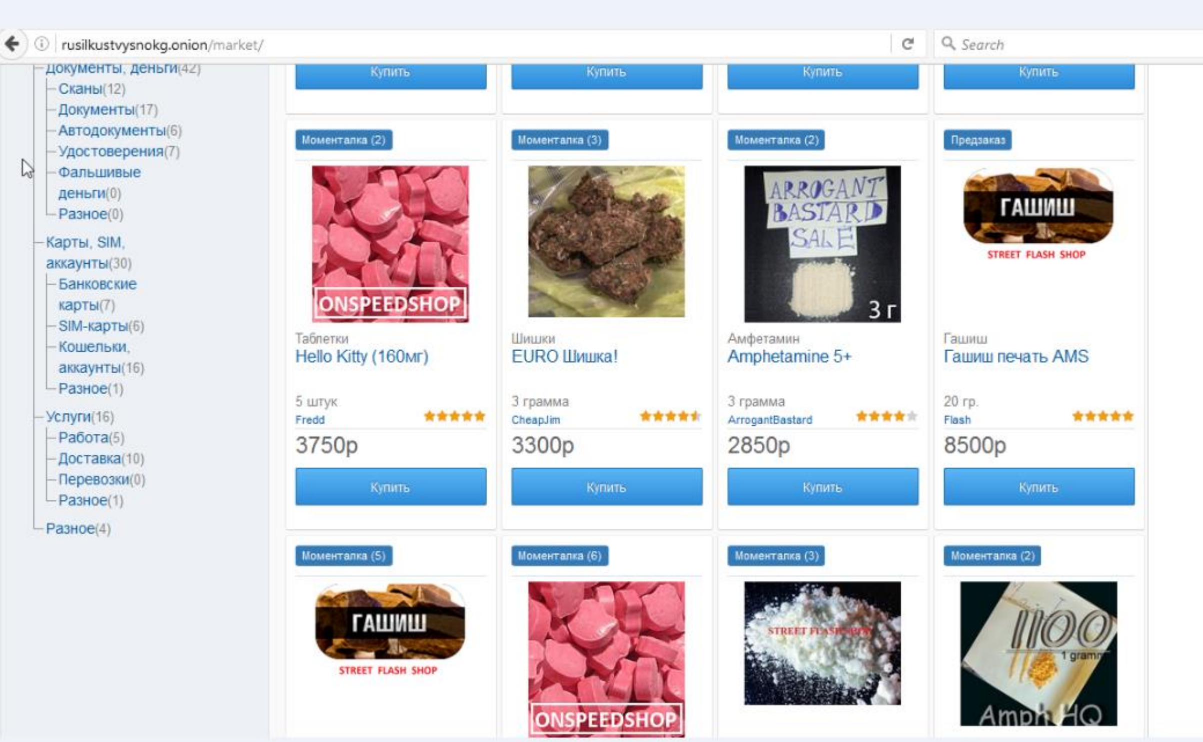
9.1.5 Evidence gained from NoAttachments.docx [NoAttachments.zip – Word – Embeddings]



to make it burn slower)

Product	Price	Quantity
Pack of 10x1ml 30-Gauge Insulin Syringes	10 USD = 0.016 $	Buy now
SAMPLER One-Point Of Heroin#4 (0.1g)	30 USD = 0.048 $	1 X Buy now
GRAND OPENING SPECIAL QUATER GRAM HEROIN#4 (0.25g)	55 USD = 0.088 $	1 X Buy now
HALF GRAM HEROIN#4 (0.50g)	100 USD = 0.160 $	1 X Buy now
GRAND OPENING SPECIAL FULL WEIGHED GRAM	180 USD =	1 X

9.1.6 Evidence gained from 11-220Records.xlsx [11-220Records.zip – Media – Images]



rusilkustvysnokg.onion/market/

- Документы, деньги(42)
  - Сканы(12)
  - Документы(17)
  - Автодокументы(6)
  - Удостоверения(7)
  - Фальшивые деньги(0)
  - Разное(0)
- Карты, SIM, аккаунты(30)
  - Банковские карты(7)
  - SIM-карты(6)
  - Кошельки, аккаунты(16)
  - Разное(1)
- Услуги(16)
  - Работа(5)
  - Доставка(10)
  - Перевозки(0)
  - Разное(1)
- Разное(4)

Моментапка (2)
Таблетки
Hello Kitty (160мг)
5 штук
Fredd ★★★★★
3750р

Моментапка (3)
Шишки
EURO Шишка!
3 грамма
CheapJim ★★★★★
3300р

Моментапка (2)
Амфетамин
Amphetamine 5+
3 грамма
ArrogantBastard ★★★★☆
2850р

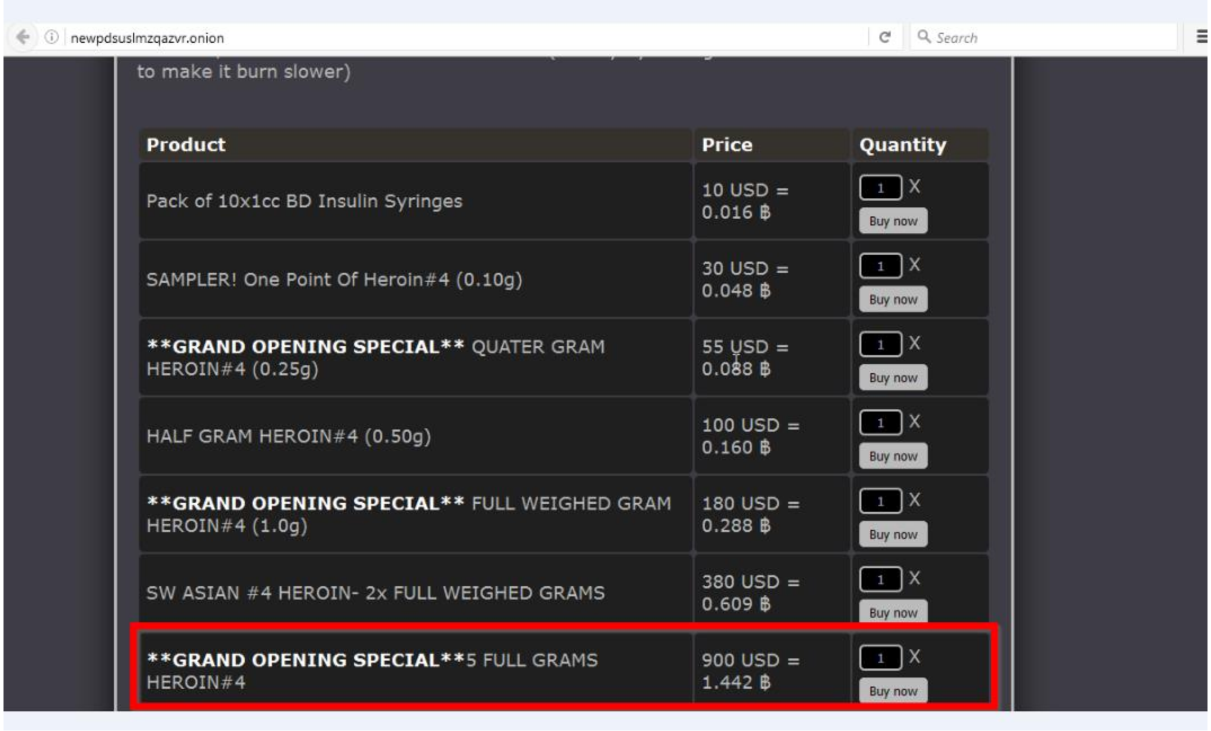
Предзаказ
Гашиш
Гашиш печать AMS
20 гр.
Flash ★★★★★
8500р

Моментапка (5)

Моментапка (6)

Моментапка (3)

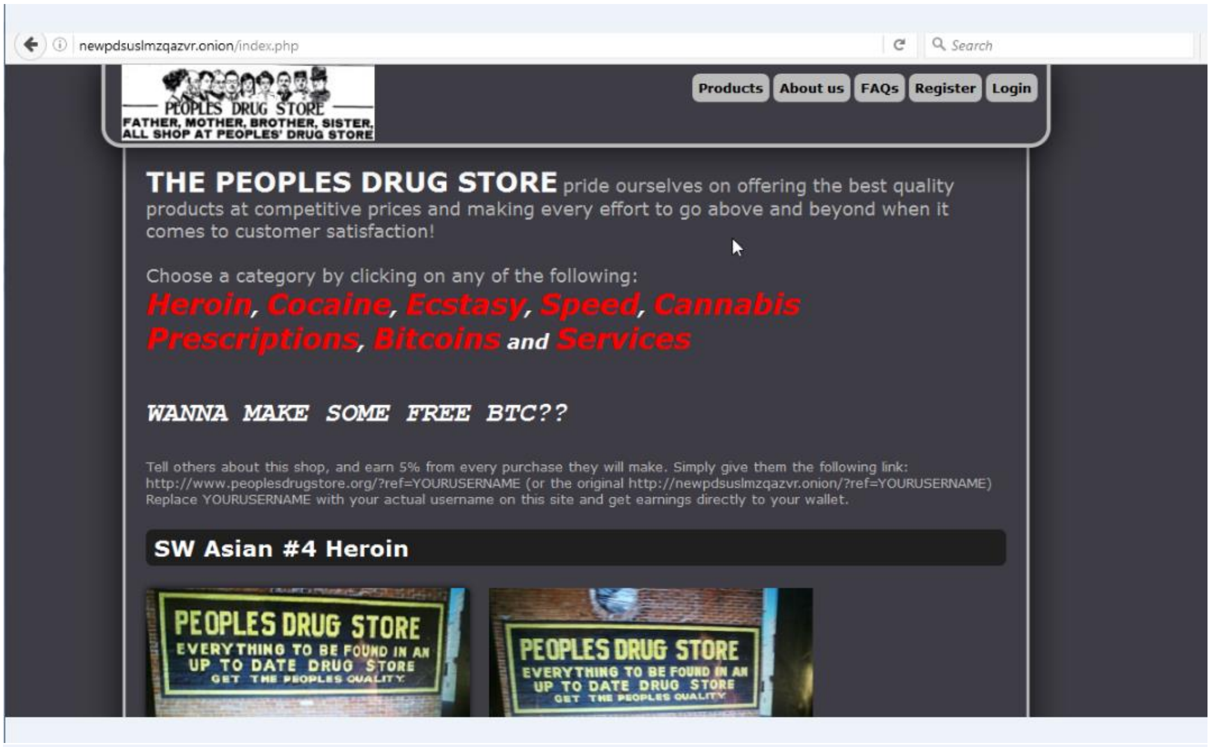
Моментапка (2)



newpdsuslmzqazvr.onion

to make it burn slower)

Product	Price	Quantity
Pack of 10x1cc BD Insulin Syringes	10 USD = 0.016 ฿	1 X Buy now
SAMPLER! One Point Of Heroin#4 (0.10g)	30 USD = 0.048 ฿	1 X Buy now
****GRAND OPENING SPECIAL**** QUATER GRAM HEROIN#4 (0.25g)	55 USD = 0.088 ฿	1 X Buy now
HALF GRAM HEROIN#4 (0.50g)	100 USD = 0.160 ฿	1 X Buy now
****GRAND OPENING SPECIAL**** FULL WEIGHED GRAM HEROIN#4 (1.0g)	180 USD = 0.288 ฿	1 X Buy now
SW ASIAN #4 HEROIN- 2x FULL WEIGHED GRAMS	380 USD = 0.609 ฿	1 X Buy now
****GRAND OPENING SPECIAL****5 FULL GRAMS HEROIN#4	900 USD = 1.442 ฿	1 X Buy now



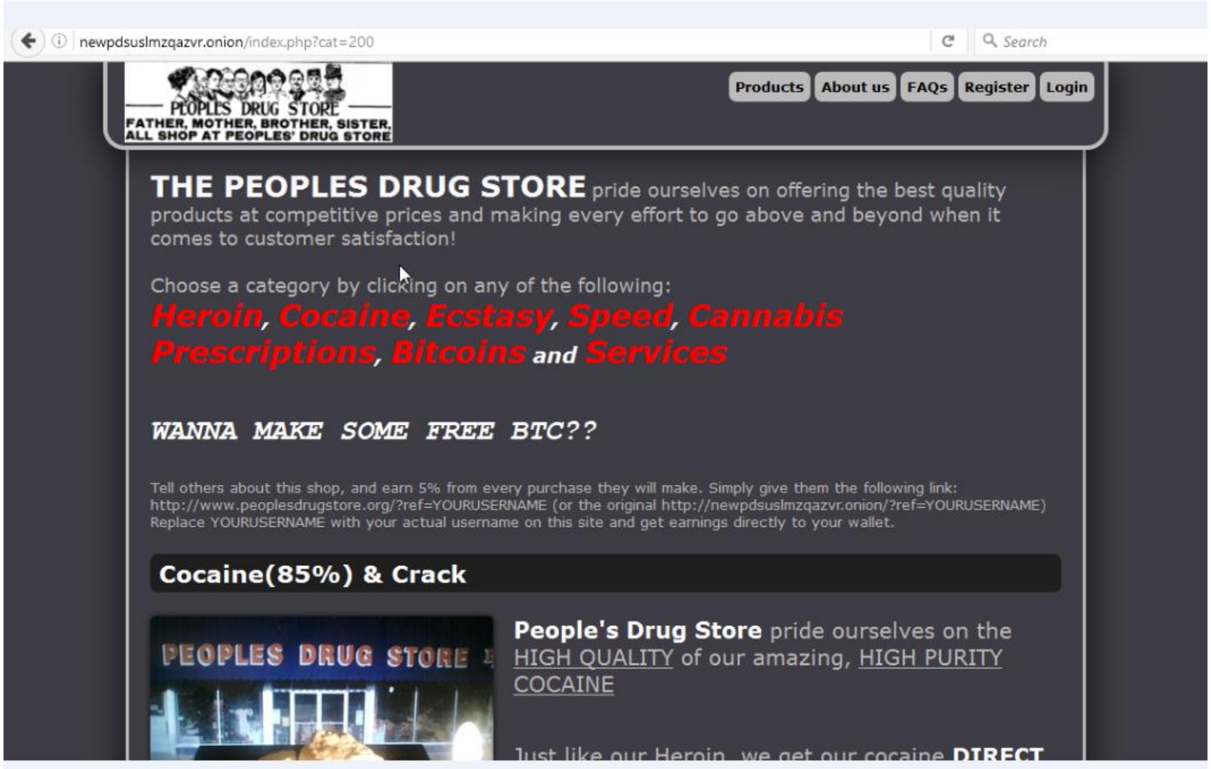
THE PEOPLES DRUG STORE pride ourselves on offering the best quality products at competitive prices and making every effort to go above and beyond when it comes to customer satisfaction!

Choose a category by clicking on any of the following:
Heroin, Cocaine, Ecstasy, Speed, Cannabis Prescriptions, Bitcoins and Services

WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 5% from every purchase they will make. Simply give them the following link:
http://www.peoplesdrugstore.org/?ref=YOURUSERNAME (or the original http://newpdsuslmzqazvr.onion/?ref=YOURUSERNAME)
Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

SW Asian #4 Heroin


newpdsuslmzqazvr.onion/index.php?cat=200
Search
PEOPLES DRUG STORE
FATHER, MOTHER, BROTHER, SISTER,
ALL SHOP AT PEOPLES' DRUG STORE
Products
About us
FAQs
Register
Login
PEOPLES DRUG STORE

THE PEOPLES DRUG STORE pride ourselves on offering the best quality products at competitive prices and making every effort to go above and beyond when it comes to customer satisfaction!

Choose a category by clicking on any of the following:
Heroin, Cocaine, Ecstasy, Speed, Cannabis Prescriptions, Bitcoins and Services

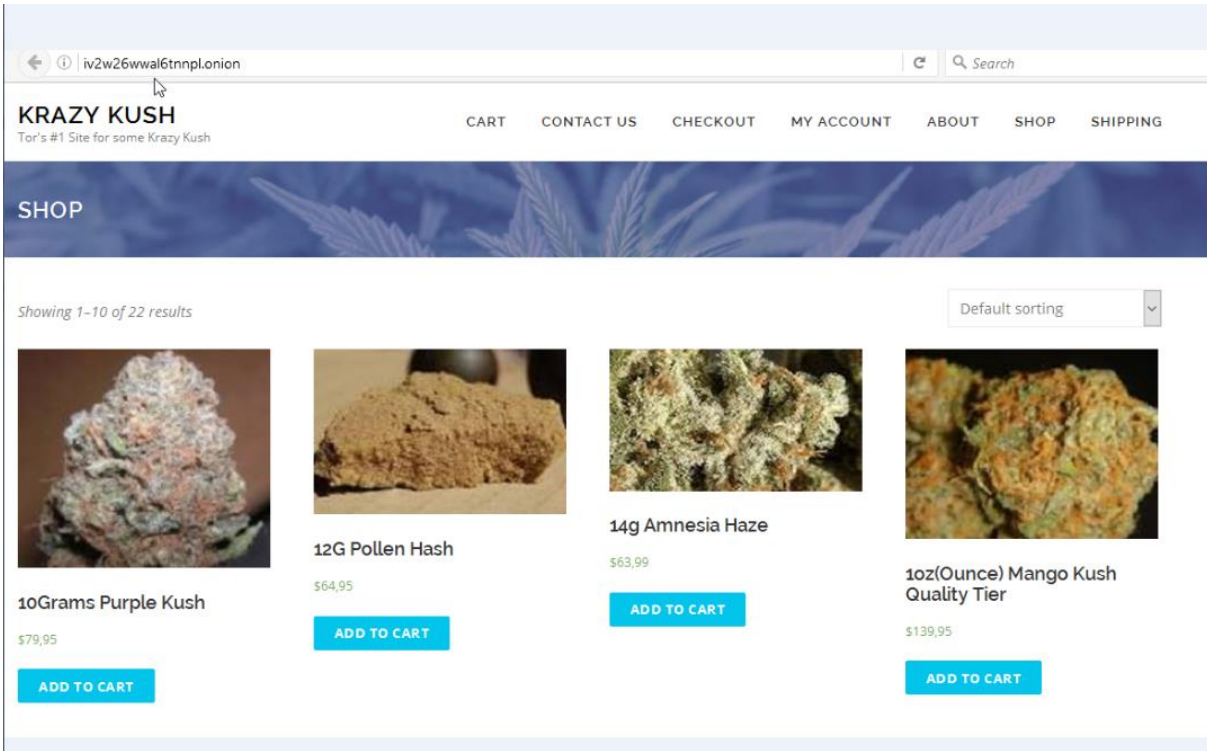
WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 5% from every purchase they will make. Simply give them the following link:
http://www.peoplesdrugstore.org/?ref=YOURUSERNAME (or the original http://newpdsuslmzqazvr.onion/?ref=YOURUSERNAME)
Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

Cocaine(85%) & Crack

People's Drug Store pride ourselves on the HIGH QUALITY of our amazing, HIGH PURITY COCAINE

Just like our Heroin, we get our cocaine **DIRECT**



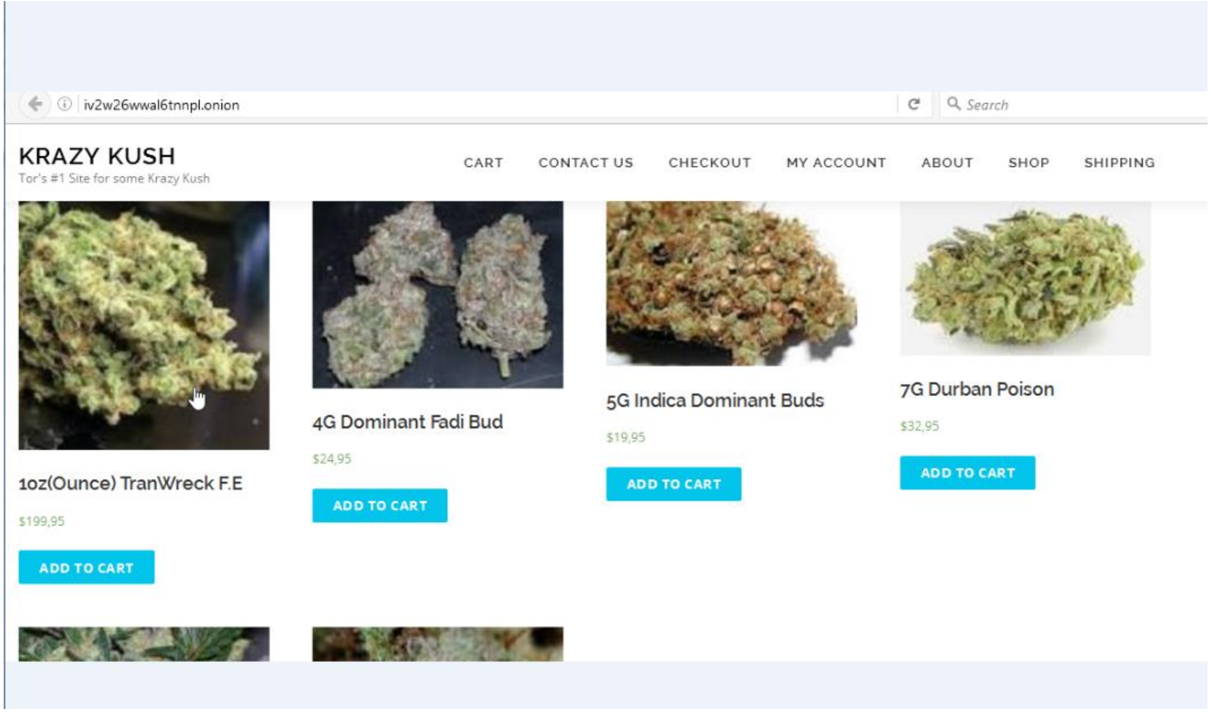
Showing 1–10 of 22 results

10Grams Purple Kush
$79,95

12G Pollen Hash
$64,95

14g Amnesia Haze
$63,99

1oz(Ounce) Mango Kush Quality Tier
$139,95

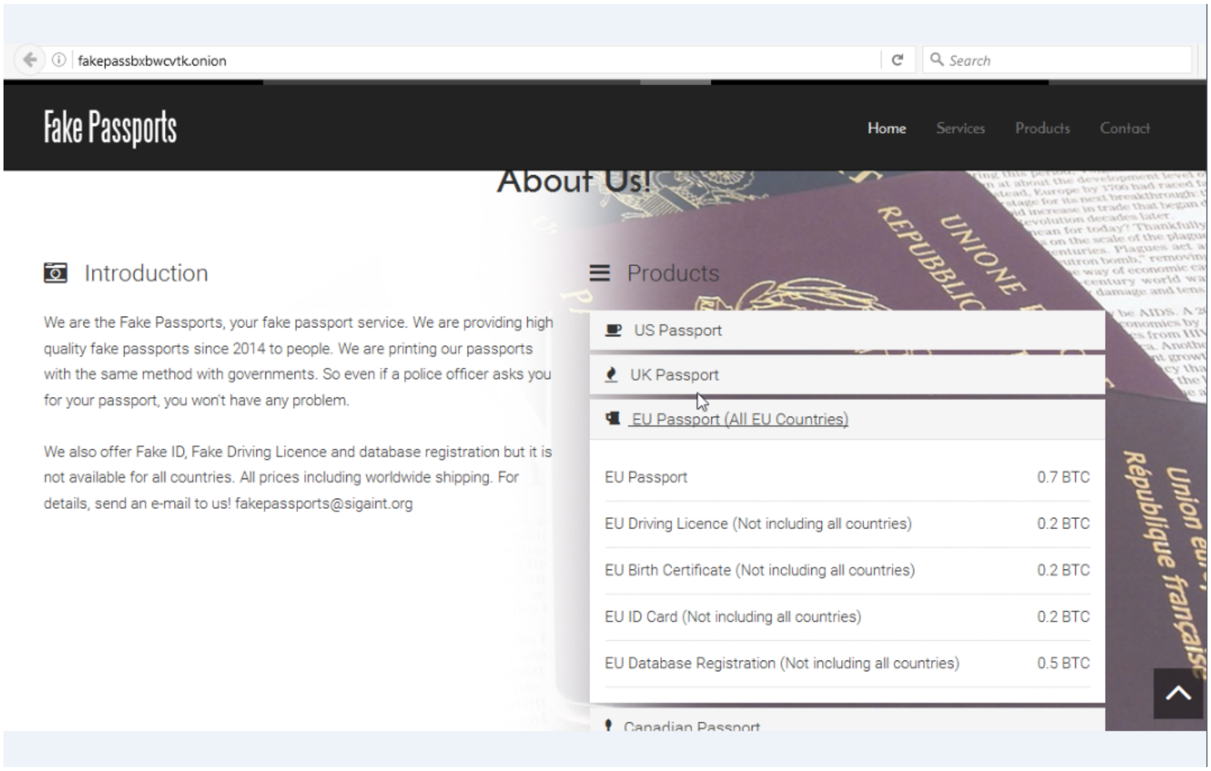


1oz(Ounce) TranWreck F.E
$199,95

4G Dominant Fadi Bud
$24,95

5G Indica Dominant Buds
$19,95

7G Durban Poison
$32,95



About Us!

Introduction

We are the Fake Passports, your fake passport service. We are providing high quality fake passports since 2014 to people. We are printing our passports with the same method with governments. So even if a police officer asks you for your passport, you won't have any problem.

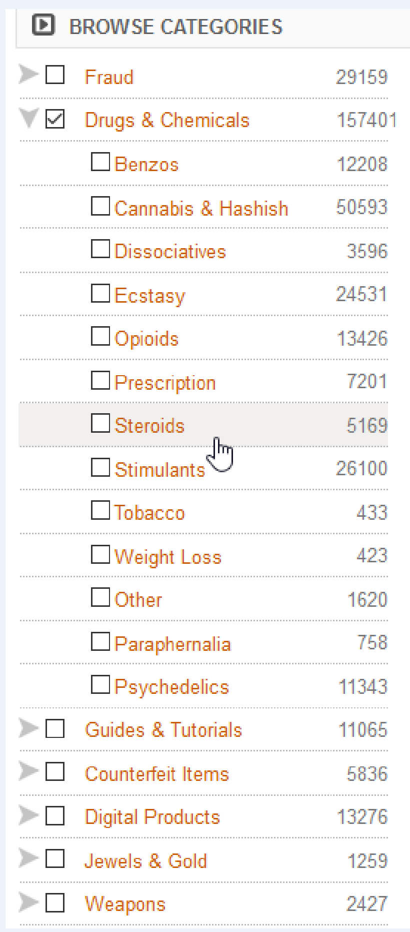
We also offer Fake ID, Fake Driving Licence and database registration but it is not available for all countries. All prices including worldwide shipping. For details, send an e-mail to us! fakepassports@sigaint.org

Products

- US Passport
- UK Passport
- EU Passport (All EU Countries)

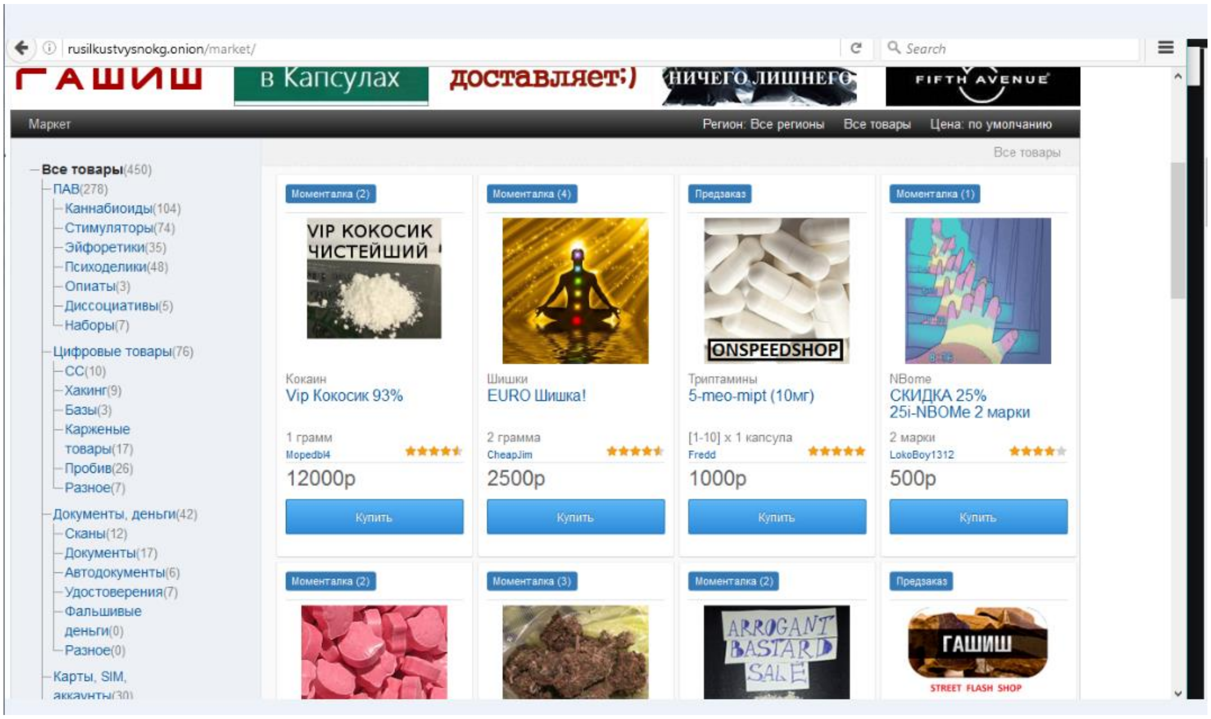
EU Passport	0.7 BTC
EU Driving Licence (Not including all countries)	0.2 BTC
EU Birth Certificate (Not including all countries)	0.2 BTC
EU ID Card (Not including all countries)	0.2 BTC
EU Database Registration (Not including all countries)	0.5 BTC

- Canadian Passport



BROWSE CATEGORIES

□ Fraud	29159
☑ Drugs & Chemicals	157401
□ Benzos	12208
□ Cannabis & Hashish	50593
□ Dissociatives	3596
□ Ecstasy	24531
□ Opioids	13426
□ Prescription	7201
□ Steroids	5169
□ Stimulants	26100
□ Tobacco	433
□ Weight Loss	423
□ Other	1620
□ Paraphernalia	758
□ Psychedelics	11343
□ Guides & Tutorials	11065
□ Counterfeit Items	5836
□ Digital Products	13276
□ Jewels & Gold	1259
□ Weapons	2427



Моменталка (2)
Кокаин
Vip Кокосик 93%
1 грамм
Mopedbl4 ★★★★★
12000р
Купить

Моменталка (4)
Шишки
EURO Шишка!
2 грамма
CheapJim ★★★★★
2500р
Купить

Предзаказ
Триптамины
5-meo-mipt (10мг)
[1-10] x 1 капсула
Fredd ★★★★★
1000р
Купить

Моменталка (1)
NBome
СКИДКА 25%
25i-NBOMe 2 марки
2 марки
LokoBoy1312 ★★★★☆
500р
Купить

Моменталка (2)

Моменталка (3)

Моменталка (2)

Предзаказ

9.1.7 Evidence gained from Katie – 1.jpg 2.jpg 3.jpg 4.jpg [WhatsAppDanielKatie.txt]

06/10/2016, 18:32 - Katie: Hey!

06/10/2016, 18:32 - Daniel McGowan: Hey babe! What happened? Why are you whatsapping me?

06/10/2016, 18:32 - Katie: Things went south last night... Tony got arrested with a care package. Cops found two keys on him. The package was for the chinese in Manchester.

06/10/2016, 18:33 - Daniel McGowan: Oh shit! What’s next? Do they have anything on us? Is Tony gonna talk?

06/10/2016, 18:33 - Katie: No, he knows the drill. He knows what happens to his family if he talks. We are clean, they won’t have anything on us. Don’t worry, we will contain this situation.

06/10/2016, 18:34 - Daniel McGowan: Better be, we’ve got a lot hanging on our relationship with the chinese. They are the only ones that have good market established in the underground. We need to maintain this trade deal, otherwise we are not going to reach our endgame, you know that.

06/10/2016, 18:34 - Daniel McGowan: We have to find someone else who can keep things going with the chinese trade and possibly have a role in an endgame.

06/10/2016, 18:34 - Katie: I’m not sure about involving strangers without vetting. We need someone we trust to do the Hamburg job. We’ve already got the plan confirmed at the table. We cannot miss the deadline.

06/10/2016, 18:34 - Daniel McGowan: I know but we will have to take a risk. We have only one shot at the G20. Do you know any animal lovers?

06/10/2016, 18:35 - Katie: Yeah I might know one guy. He’s all into animal care and shit but he’s a boy scout. We could set him up with the chinese and keep in control for the end game.

06/10/2016, 18:35 - Daniel McGowan: Sounds good. Could you set up a meet?

06/10/2016, 18:35 - Katie: That won’t be too complicated. I could invite him to the party on saturday, so you can meet him.

06/10/2016, 18:35 - Daniel McGowan: Cool, do it. I will get him involved with the group and set him up for the chinese first. Will see how it goes after that.

09/10/2016, 11:36 - Katie: How was yesterday? Is he any good? Up for the job?

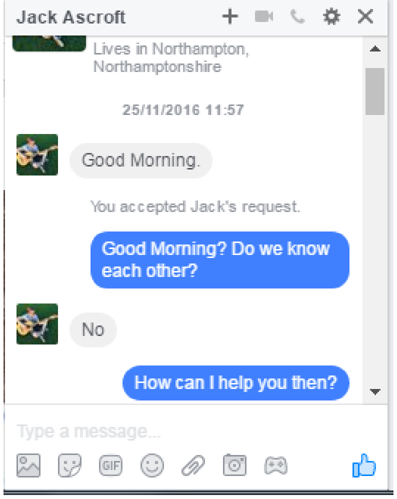
09/10/2016, 11:36 - Daniel McGowan: Yeah he looks alright. You were right, he cares about the greater good for animals though he’s a good samaritan which might cause a problem. We’ve got to change that. I’ve invited him to the protest with the others on Tuesday. I’ll set him for the stay in police station and offer to pay his bills after he loses his job.

09/10/2016, 11:36 - Katie: Isn’t that a bit too far?

09/10/2016, 11:36 - Daniel McGowan: Well you are the one that wanted a proper vetting process :) We’ve got this guy set up and desperate for the money. He is fit for the job in Hamburg and, unlike us, he doesn’t have any records. He can travel freely without getting picked up. We need this guy.

09/10/2016, 11:38 - Katie: I guess you are right.

9.1.8 Evidence gained from Facebook [Hans Murschenhofer chat with Jack Ascroft]



Jack Ascroft

Lives in Northampton, Northamptonshire

25/11/2016 11:57

Good Morning.

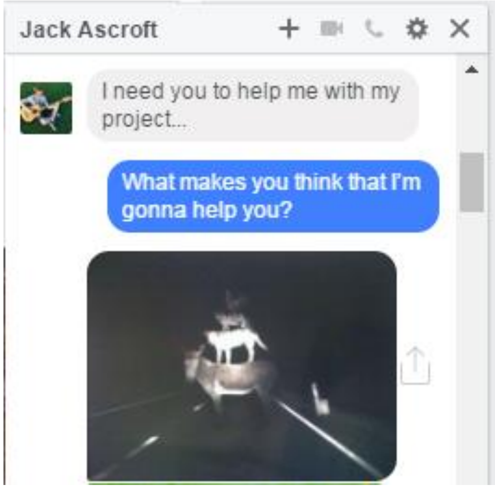
You accepted Jack's request.

Good Morning? Do we know each other?

No

How can I help you then?

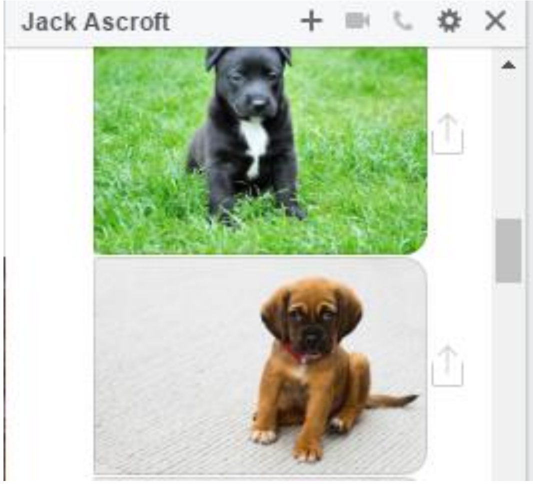
Type a message...



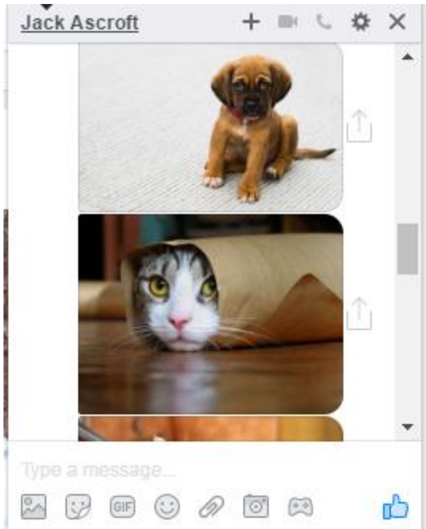
Jack Ascroft

I need you to help me with my project...

What makes you think that I'm gonna help you?

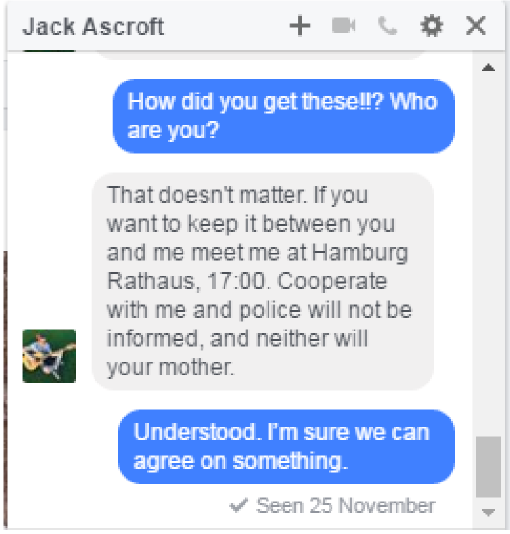


Jack Ascroft



Jack Ascroft

Type a message...



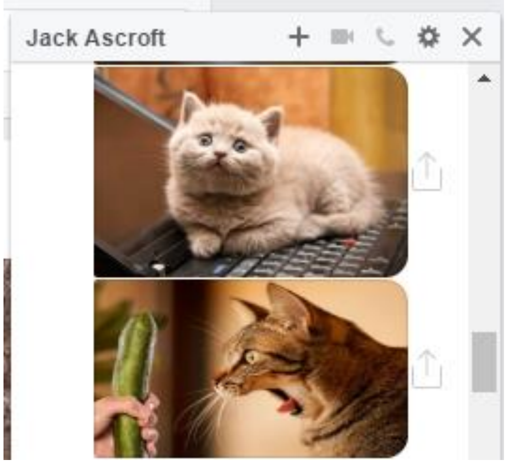
Jack Ascroft

How did you get these!!? Who are you?

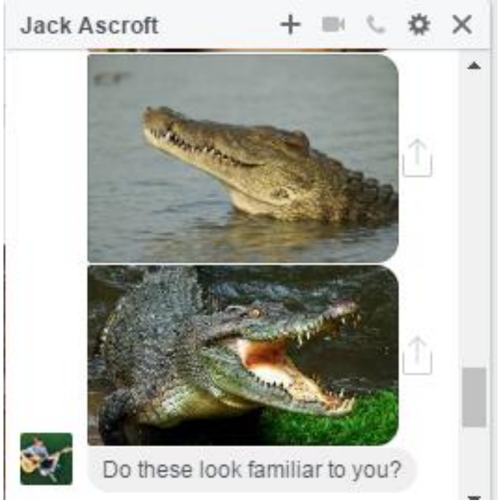
That doesn't matter. If you want to keep it between you and me meet me at Hamburg Rathaus, 17:00. Cooperate with me and police will not be informed, and neither will your mother.

Understood. I'm sure we can agree on something.

✓ Seen 25 November



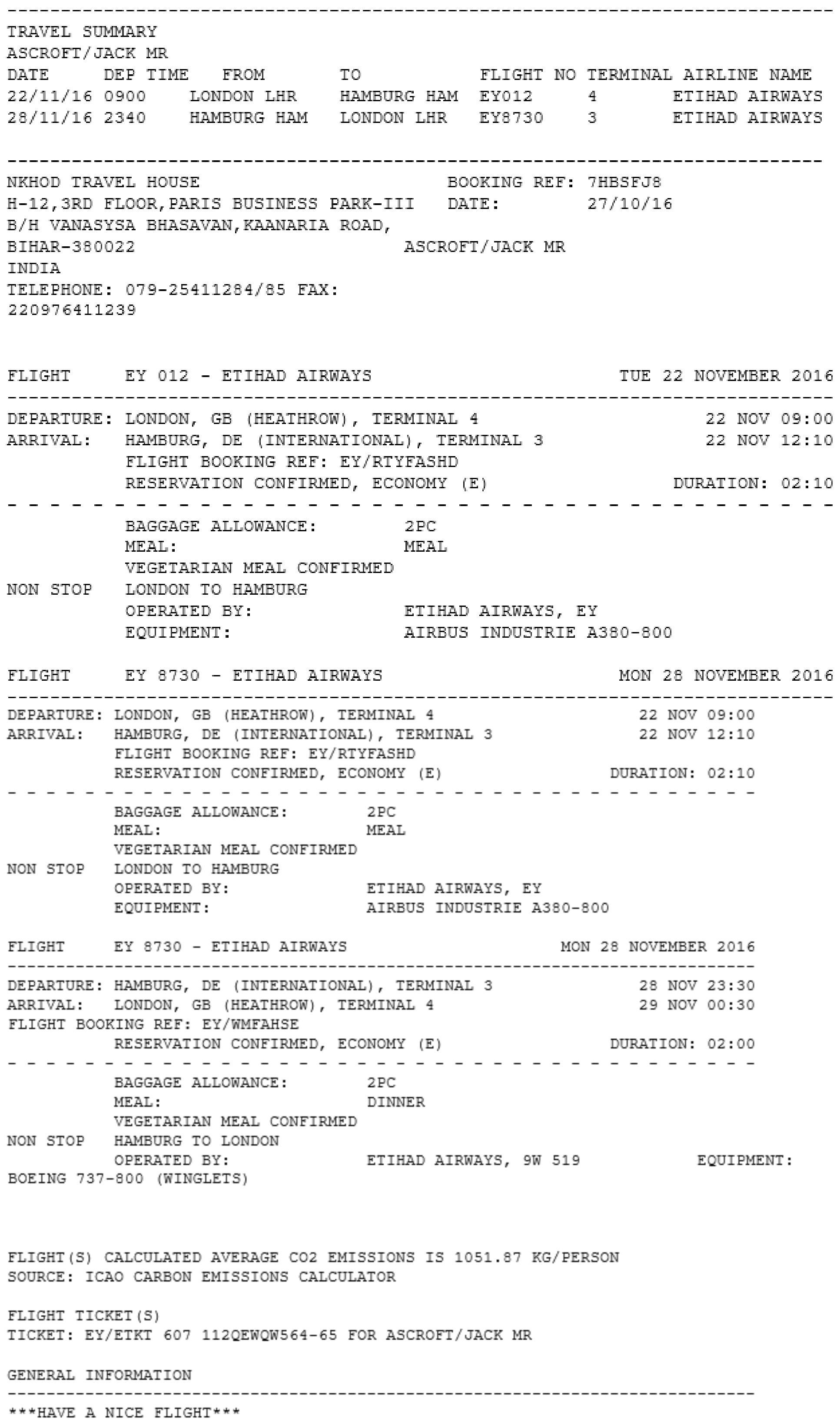
Jack Ascroft



Jack Ascroft

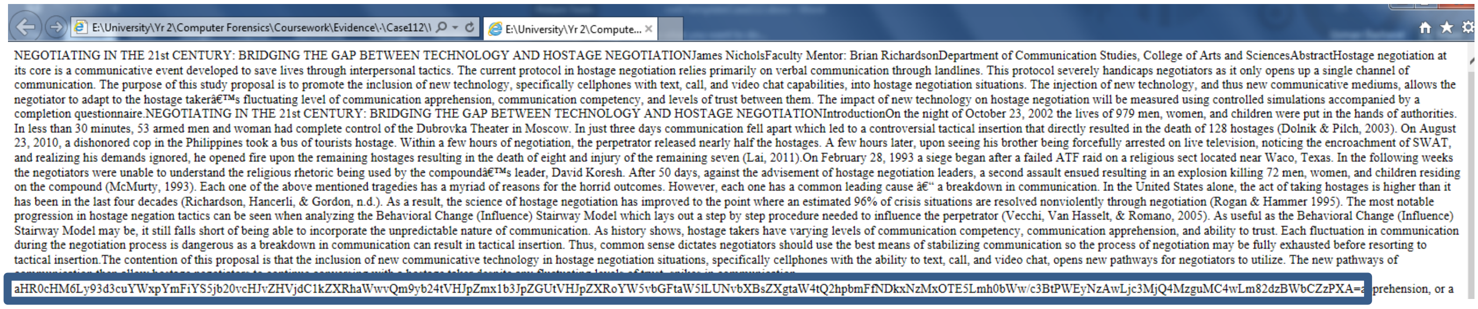
Do these look familiar to you?

9.1.9 Evidence gained from NKHOD Travel.PDF [NKHOD Travel.PDF]



```
------------------------------------------------------------------------------
TRAVEL SUMMARY
ASCROFT/JACK MR
DATE     DEP TIME   FROM       TO           FLIGHT NO TERMINAL AIRLINE NAME
22/11/16 0900    LONDON LHR    HAMBURG HAM  EY012      4       ETIHAD AIRWAYS
28/11/16 2340    HAMBURG HAM   LONDON LHR   EY8730     3       ETIHAD AIRWAYS

-----------------------------------------------------------------------------
NKHOD TRAVEL HOUSE                             BOOKING REF: 7HBSFJ8
H-12,3RD FLOOR,PARIS BUSINESS PARK-III   DATE:        27/10/16
B/H VANASYSA BHASAVAN,KAANARIA ROAD,
BIHAR-380022                         ASCROFT/JACK MR
INDIA
TELEPHONE: 079-25411284/85 FAX:
220976411239


FLIGHT     EY 012 - ETIHAD AIRWAYS                         TUE 22 NOVEMBER 2016
------------------------------------------------------------------------------
DEPARTURE: LONDON, GB (HEATHROW), TERMINAL 4                        22 NOV 09:00
ARRIVAL:   HAMBURG, DE (INTERNATIONAL), TERMINAL 3                  22 NOV 12:10
           FLIGHT BOOKING REF: EY/RTYFASHD
           RESERVATION CONFIRMED, ECONOMY (E)                  DURATION: 02:10
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
           BAGGAGE ALLOWANCE:         2PC
           MEAL:                      MEAL
           VEGETARIAN MEAL CONFIRMED
NON STOP   LONDON TO HAMBURG
           OPERATED BY:               ETIHAD AIRWAYS, EY
           EQUIPMENT:                 AIRBUS INDUSTRIE A380-800

FLIGHT     EY 8730 - ETIHAD AIRWAYS                        MON 28 NOVEMBER 2016
------------------------------------------------------------------------------
DEPARTURE: LONDON, GB (HEATHROW), TERMINAL 4                   22 NOV 09:00
ARRIVAL:   HAMBURG, DE (INTERNATIONAL), TERMINAL 3             22 NOV 12:10
           FLIGHT BOOKING REF: EY/RTYFASHD
           RESERVATION CONFIRMED, ECONOMY (E)             DURATION: 02:10
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
           BAGGAGE ALLOWANCE:        2PC
           MEAL:                     MEAL
           VEGETARIAN MEAL CONFIRMED
NON STOP   LONDON TO HAMBURG
           OPERATED BY:              ETIHAD AIRWAYS, EY
           EQUIPMENT:                AIRBUS INDUSTRIE A380-800

FLIGHT     EY 8730 - ETIHAD AIRWAYS                   MON 28 NOVEMBER 2016
---------------------------------------------------------------------------
DEPARTURE: HAMBURG, DE (INTERNATIONAL), TERMINAL 3             28 NOV 23:30
ARRIVAL:   LONDON, GB (HEATHROW), TERMINAL 4                   29 NOV 00:30
FLIGHT BOOKING REF: EY/WMFAHSE
           RESERVATION CONFIRMED, ECONOMY (E)             DURATION: 02:00
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
           BAGGAGE ALLOWANCE:        2PC
           MEAL:                     DINNER
           VEGETARIAN MEAL CONFIRMED
NON STOP   HAMBURG TO LONDON
           OPERATED BY:              ETIHAD AIRWAYS, 9W 519          EQUIPMENT:
BOEING 737-800 (WINGLETS)


FLIGHT(S) CALCULATED AVERAGE CO2 EMISSIONS IS 1051.87 KG/PERSON
SOURCE: ICAO CARBON EMISSIONS CALCULATOR

FLIGHT TICKET(S)
TICKET: EY/ETKT 607 112QEWQW564-65 FOR ASCROFT/JACK MR

GENERAL INFORMATION
---------------------------------------------------------------------------
***HAVE A NICE FLIGHT***
```

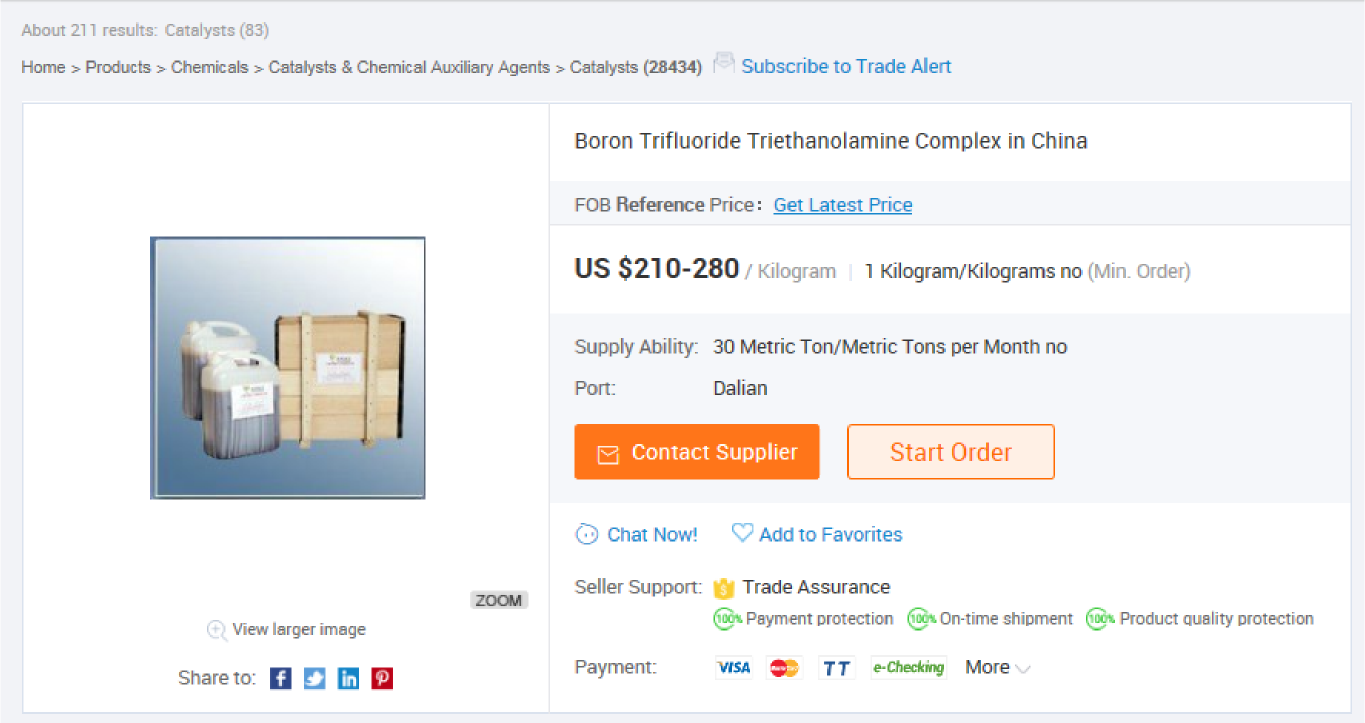
9.1.10 Evidence gained from NoAttachments.docx [NoAttachments.zip – Word - Document.xml to Document.HTML]


E:\University\Yr 2\Computer Forensics\Coursework\Evidence\-\Case112\\
E:\University\Yr 2\Compute...

NEGOTIATING IN THE 21st CENTURY: BRIDGING THE GAP BETWEEN TECHNOLOGY AND HOSTAGE NEGOTIATIONJames NicholsFaculty Mentor: Brian RichardsonDepartment of Communication Studies, College of Arts and SciencesAbstractHostage negotiation at its core is a communicative event developed to save lives through interpersonal tactics. The current protocol in hostage negotiation relies primarily on verbal communication through landlines. This protocol severely handicaps negotiators as it only opens up a single channel of communication. The purpose of this study proposal is to promote the inclusion of new technology, specifically cellphones with text, call, and video chat capabilities, into hostage negotiation situations. The injection of new technology, and thus new communicative mediums, allows the negotiator to adapt to the hostage takerâ€™s fluctuating level of communication apprehension, communication competency, and levels of trust between them. The impact of new technology on hostage negotiation will be measured using controlled simulations accompanied by a completion questionnaire.NEGOTIATING IN THE 21st CENTURY: BRIDGING THE GAP BETWEEN TECHNOLOGY AND HOSTAGE NEGOTIATIONIntroductionOn the night of October 23, 2002 the lives of 979 men, women, and children were put in the hands of authorities. In less than 30 minutes, 53 armed men and woman had complete control of the Dubrovka Theater in Moscow. In just three days communication fell apart which led to a controversial tactical insertion that directly resulted in the death of 128 hostages (Dolnik & Pilch, 2003). On August 23, 2010, a dishonored cop in the Philippines took a bus of tourists hostage. Within a few hours of negotiation, the perpetrator released nearly half the hostages. A few hours later, upon seeing his brother being forcefully arrested on live television, noticing the encroachment of SWAT, and realizing his demands ignored, he opened fire upon the remaining hostages resulting in the death of eight and injury of the remaining seven (Lai, 2011).On February 28, 1993 a siege began after a failed ATF raid on a religious sect located near Waco, Texas. In the following weeks the negotiators were unable to understand the religious rhetoric being used by the compoundâ€™s leader, David Koresh. After 50 days, against the advisement of hostage negotiation leaders, a second assault ensued resulting in an explosion killing 72 men, women, and children residing on the compound (McMurty, 1993). Each one of the above mentioned tragedies has a myriad of reasons for the horrid outcomes. However, each one has a common leading cause â€“ a breakdown in communication. In the United States alone, the act of taking hostages is higher than it has been in the last four decades (Richardson, Hancerli, & Gordon, n.d.). As a result, the science of hostage negotiation has improved to the point where an estimated 96% of crisis situations are resolved nonviolently through negotiation (Rogan & Hammer 1995). The most notable progression in hostage negation tactics can be seen when analyzing the Behavioral Change (Influence) Stairway Model which lays out a step by step procedure needed to influence the perpetrator (Vecchi, Van Hasselt, & Romano, 2005). As useful as the Behavioral Change (Influence) Stairway Model may be, it still falls short of being able to incorporate the unpredictable nature of communication. As history shows, hostage takers have varying levels of communication competency, communication apprehension, and ability to trust. Each fluctuation in communication during the negotiation process is dangerous as a breakdown in communication can result in tactical insertion. Thus, common sense dictates negotiators should use the best means of stabilizing communication so the process of negotiation may be fully exhausted before resorting to tactical insertion.The contention of this proposal is that the inclusion of new communicative technology in hostage negotiation situations, specifically cellphones with the ability to text, call, and video chat, opens new pathways for negotiators to utilize. The new pathways of communication then allow hostage negotiators to continue conversing with a hostage taker despite any fluctuating levels of trust, spikes in communication

aHR0cHM6Ly93d3cuYWxpYmFiYS5jb20vcHJvZHVjdC1kZXRhaWwvQm9yb24tVHJpZmx1b3JpZGUtVHJpZXRoYW5vbGFtaW5lLUNvbXBsZXgtaW4tQ2hpbmFfNDkxNzMxOTE5Lmh0bWw/c3BtPWEyNzAwLjc3MjQ4MzguMC4wLm82dzBWbCZzPXA= apprehension, or a

Converted from Base64 to UTF-8: https://www.alibaba.com/product-detail/Boron-Trifluoride-Triethanolamine-Complex-in-China_491731919.html?spm=a2700.7724838.0.0.o6w0Vl&s=p



About 211 results: Catalysts (83)

Home > Products > Chemicals > Catalysts & Chemical Auxiliary Agents > Catalysts (28434) Subscribe to Trade Alert

Boron Trifluoride Triethanolamine Complex in China

FOB Reference Price: Get Latest Price

US $210-280 / Kilogram | 1 Kilogram/Kilograms no (Min. Order)

Supply Ability: 30 Metric Ton/Metric Tons per Month no

Port: Dalian

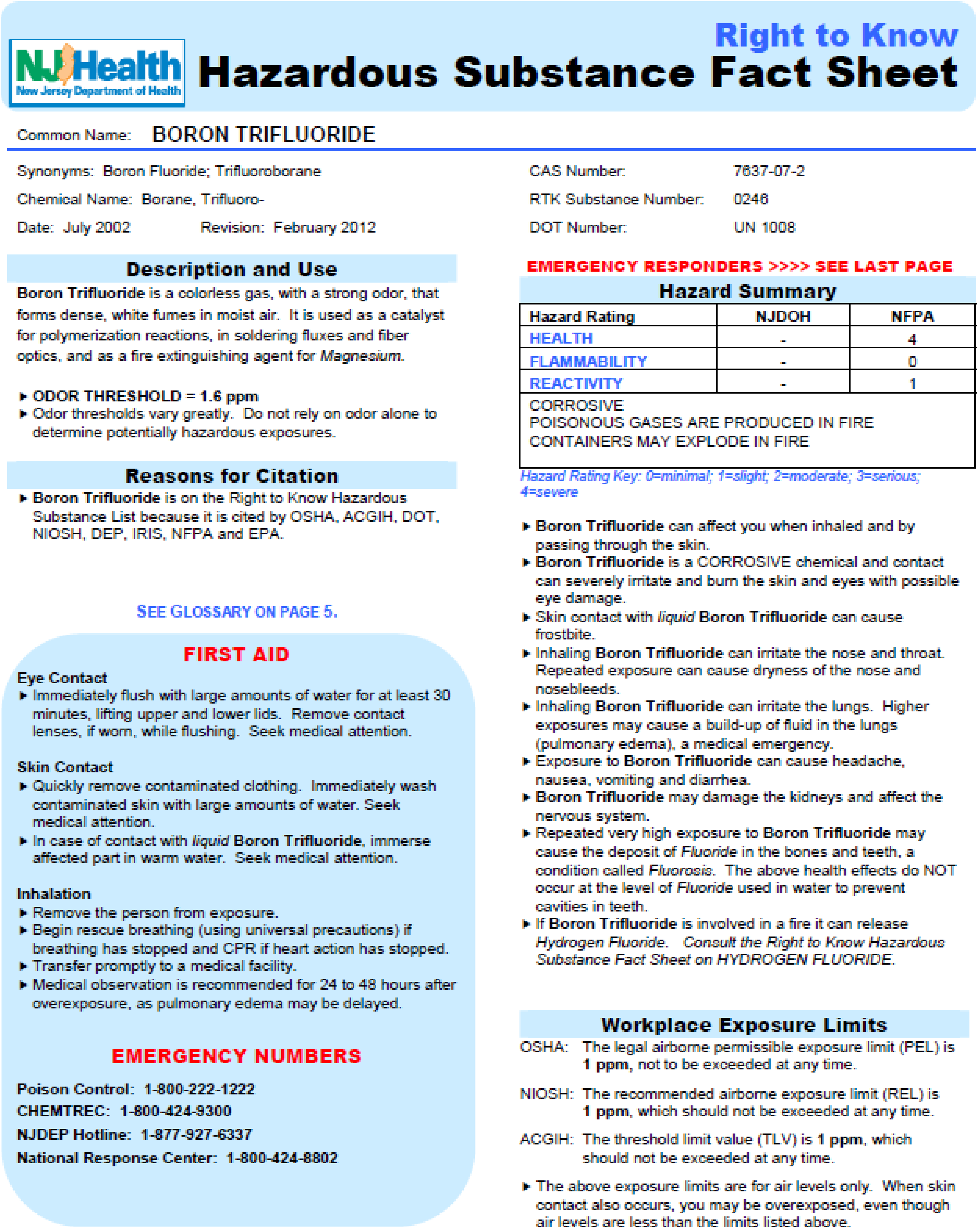
Seller Support: Trade Assurance

100% Payment protection 100% On-time shipment 100% Product quality protection

Payment:

Link above lead me to this site.

9.1.11 Evidence gained from Boron Trifluoride.GIF [Boron Trifluoride.PDF pg.1 to pg4. pg1 displayed]



Right to Know

NJ Health
New Jersey Department of Health

Hazardous Substance Fact Sheet

Common Name: BORON TRIFLUORIDE

Synonyms: Boron Fluoride; Trifluoroborane

Chemical Name: Borane, Trifluoro-

Date: July 2002 Revision: February 2012

CAS Number:	7637-07-2
RTK Substance Number:	0246
DOT Number:	UN 1008

Description and Use

Boron Trifluoride is a colorless gas, with a strong odor, that forms dense, white fumes in moist air. It is used as a catalyst for polymerization reactions, in soldering fluxes and fiber optics, and as a fire extinguishing agent for *Magnesium*.

- **ODOR THRESHOLD = 1.6 ppm**
- Odor thresholds vary greatly. Do not rely on odor alone to determine potentially hazardous exposures.

Reasons for Citation

- **Boron Trifluoride** is on the Right to Know Hazardous Substance List because it is cited by OSHA, ACGIH, DOT, NIOSH, DEP, IRIS, NFPA and EPA.

SEE GLOSSARY ON PAGE 5.

FIRST AID

Eye Contact

- Immediately flush with large amounts of water for at least 30 minutes, lifting upper and lower lids. Remove contact lenses, if worn, while flushing. Seek medical attention.

Skin Contact

- Quickly remove contaminated clothing. Immediately wash contaminated skin with large amounts of water. Seek medical attention.
- In case of contact with *liquid* **Boron Trifluoride**, immerse affected part in warm water. Seek medical attention.

Inhalation

- Remove the person from exposure.
- Begin rescue breathing (using universal precautions) if breathing has stopped and CPR if heart action has stopped.
- Transfer promptly to a medical facility.
- Medical observation is recommended for 24 to 48 hours after overexposure, as pulmonary edema may be delayed.

EMERGENCY NUMBERS

Poison Control: 1-800-222-1222
CHEMTREC: 1-800-424-9300
NJDEP Hotline: 1-877-927-6337
National Response Center: 1-800-424-8802

EMERGENCY RESPONDERS >>>> SEE LAST PAGE

Hazard Summary

Hazard Rating	NJDOH	NFPA
HEALTH	-	4
FLAMMABILITY	-	0
REACTIVITY	-	1

CORROSIVE
POISONOUS GASES ARE PRODUCED IN FIRE
CONTAINERS MAY EXPLODE IN FIRE

Hazard Rating Key: 0=minimal; 1=slight; 2=moderate; 3=serious; 4=severe

- **Boron Trifluoride** can affect you when inhaled and by passing through the skin.
- **Boron Trifluoride** is a CORROSIVE chemical and contact can severely irritate and burn the skin and eyes with possible eye damage.
- Skin contact with *liquid* **Boron Trifluoride** can cause frostbite.
- Inhaling **Boron Trifluoride** can irritate the nose and throat. Repeated exposure can cause dryness of the nose and nosebleeds.
- Inhaling **Boron Trifluoride** can irritate the lungs. Higher exposures may cause a build-up of fluid in the lungs (pulmonary edema), a medical emergency.
- Exposure to **Boron Trifluoride** can cause headache, nausea, vomiting and diarrhea.
- **Boron Trifluoride** may damage the kidneys and affect the nervous system.
- Repeated very high exposure to **Boron Trifluoride** may cause the deposit of *Fluoride* in the bones and teeth, a condition called *Fluorosis*. The above health effects do NOT occur at the level of *Fluoride* used in water to prevent cavities in teeth.
- If **Boron Trifluoride** is involved in a fire it can release *Hydrogen Fluoride. Consult the Right to Know Hazardous Substance Fact Sheet on HYDROGEN FLUORIDE.*

Workplace Exposure Limits

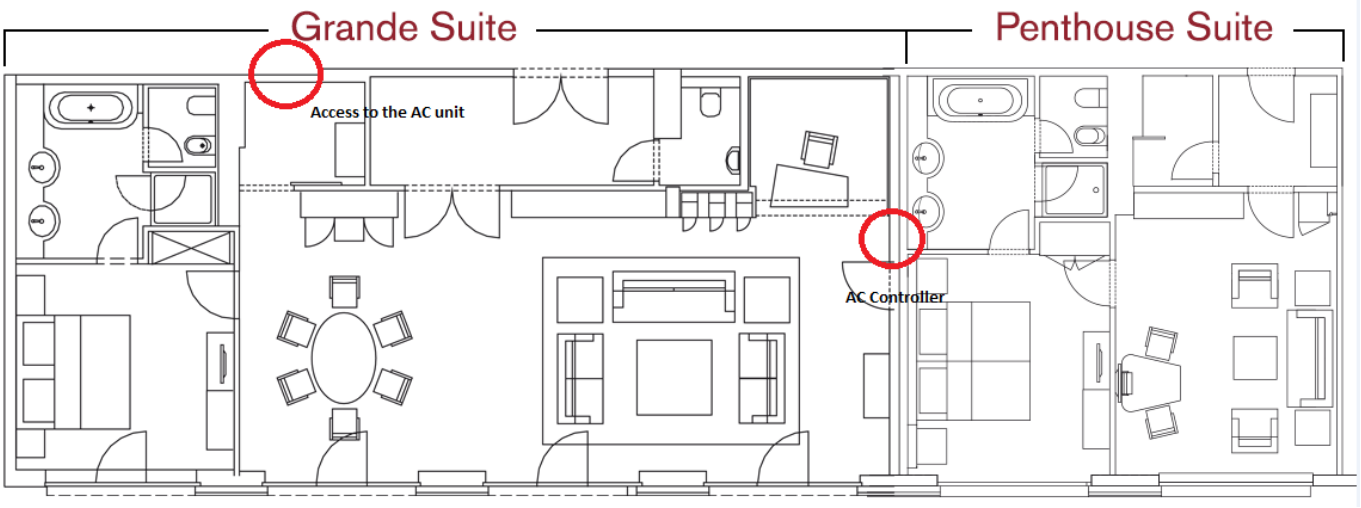
OSHA: The legal airborne permissible exposure limit (PEL) is **1 ppm**, not to be exceeded at any time.

NIOSH: The recommended airborne exposure limit (REL) is **1 ppm**, which should not be exceeded at any time.

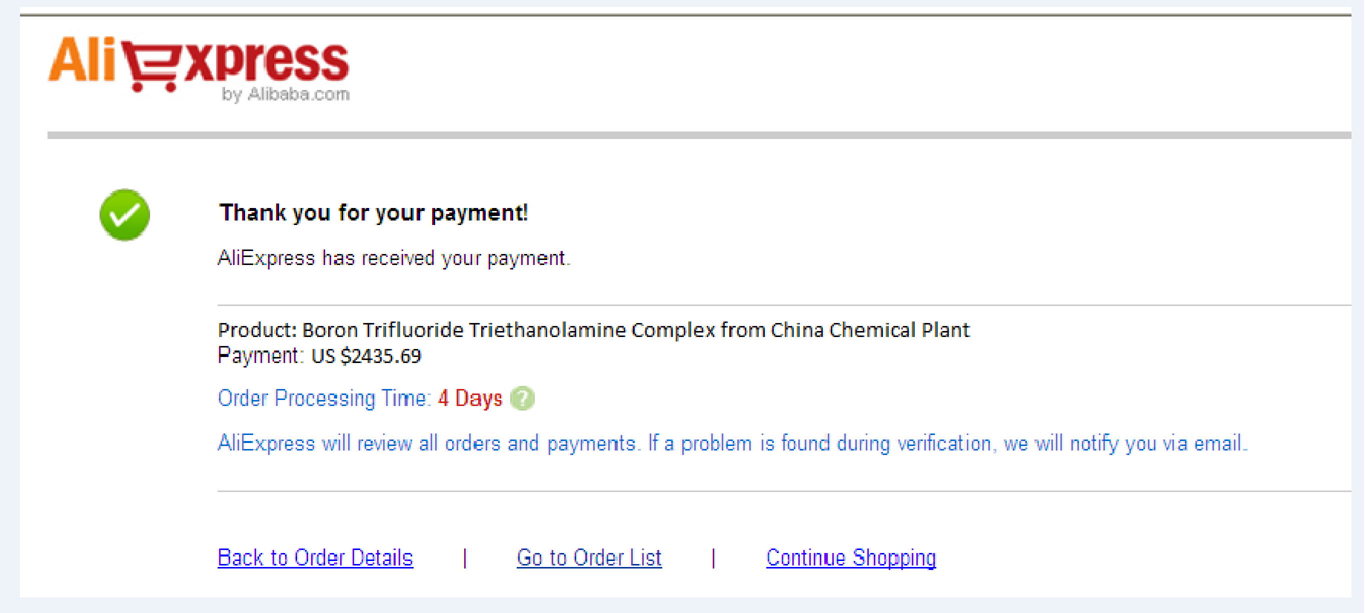
ACGIH: The threshold limit value (TLV) is **1 ppm**, which should not be exceeded at any time.

- The above exposure limits are for air levels only. When skin contact also occurs, you may be overexposed, even though air levels are less than the limits listed above.

9.1.12 Evidence gained from WhatsApp Received [Grand-Suite-Grundriss.png]



9.1.13 Evidence gained from *Nach* Folder using OpenPuff [20160606_145154.jpg, 20160606_152929.jpg, 20160606_153214.jpg, vedett-dm2wheels7201.mp4]


AliExpress by Alibaba.com

Thank you for your payment!

AliExpress has received your payment.

Product: Boron Trifluoride Triethanolamine Complex from China Chemical Plant
Payment: US $2435.69

Order Processing Time: 4 Days

AliExpress will review all orders and payments. If a problem is found during verification, we will notify you via email.

Back to Order Details | Go to Order List | Continue Shopping

9.1.14 Evidence gained from Katie to Wang.eml [Katie to Wang.eml]

On 19/08/2016 12:47 PM, wang wok chok wrote:

Yes

On 18/08/2016 21:23, Katie smartgirl wrote:

Alright, 7% it is. We've got 5 kilos of Heroin, at $113.7 a gram that's $568,500 in total.

We'll send half a kilo at a time, the first shipment in a couple days to the usual place, please make payment to the usual account on delivery.

Is that all in ok?

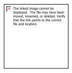
Katie

On 13/08/2016 9:21 PM, wang wok chok wrote:

Fine. 7%, but no more.

On 13/08/2016 21:17, Katie smartgirl wrote:

I've seen how much the Russians are charging, if you're not willing to pay more we'll go where we're more needed.



The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

On 11/08/2016 9:16 PM, wang wok chok wrote:

No way are we going to pay 10% more than last time, we'll give you a 3% increase.

On 07/08/2016 21:15, Katie smartgirl wrote:

Hi Wang,

Prices are increasing everywhere you know this. We're going to need a 10% increase in price.

Katie

On 07/08/2016 6:01 AM, wang wok chok wrote:

Hi Katie,
Yes, perfect timing, we could do with a new shipment now. Same deal as the past?
Wang

On 06/08/2016 18:00, Katie smartgirl wrote:

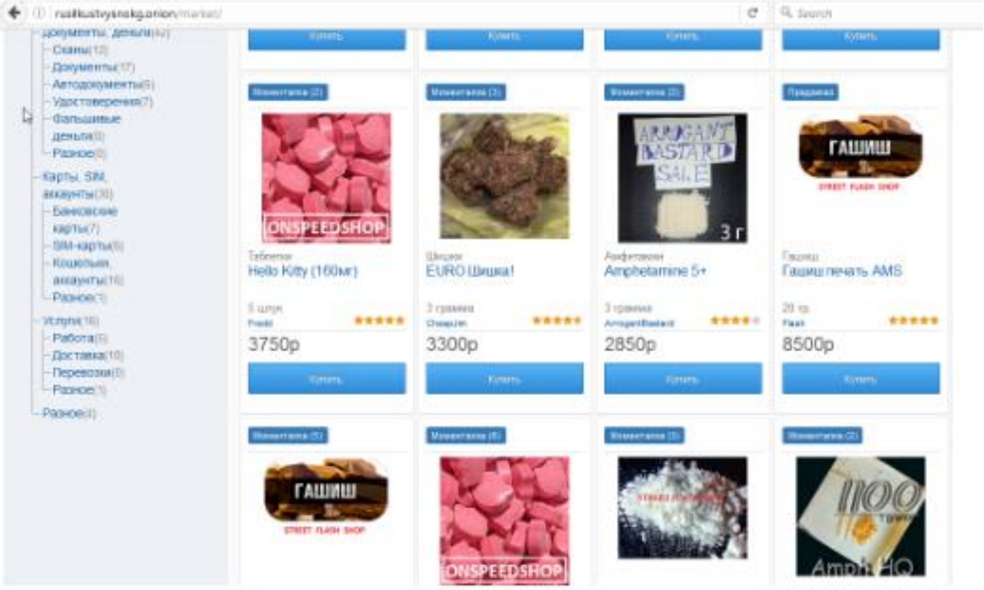
Hello Mr Wang,

We've recently come across some new supplies through our usual contact.

Are you interested? I've noticed the store's still up so I assume you're still happy to buy from us.

Katie

9.1.15 Evidence gained from Katie to Wang.eml [Attached Image]



10. TIMELINE

Date	What happened	Evidence
05/08/2016	Katie emails Daniel about Chinese deal with a picture missing. (Managed to extract the missing picture, which was web site basket of drugs).	Katie to Daniel email in NoAttachments.zip file.
05/10/2016 to 6/10/2016	Tony was arrested with cops found two keys and a care package on him. Daniel and Katie want to replace him with an animal lover and searching for one that has a record clean.	The WhatsApp conversation extracted from the four pictures in Katie's folder using OpenPuff in order of 4,3,1,2 and password used from the picture with the station sign.
09/10/2016	WhatsApp conversation between Daniel and Katie talking about trying to convince that one person to help them with Hamburg job.	The WhatsApp conversation extracted from the four pictures in Katie's folder using OpenPuff in order of 4,3,1,2 and password used from the picture with the station sign.
27/10/2016	Jack booked a flight to Hamburg from 22/11/2016 and a return date of 28/11/2016.	Found in the NKHOD TRAVEL pdf document that was decrypted.
03/11/2016	Daniel was trying to contact a hacker Miko so he can find information on a specific person (Hans).	Email between Miko and Daniel in the "I need your service" email.
12/11/2016	Miko contacted Daniel via email saying that he found information for the person he was looking for (Hans).	Email between Miko and Daniel in the "I need your service" email.
22/11/2016	There is a booked room for the Grand Elyse Hotel in Hamburg from that date. Leaving date is the 28/11/2016	From the picture, "Fwd It's time for you to stay in.jpg".
25/11/2016	Facebook conversation between Jack Ascroft and Hans Murschenhofer. Jack is blackmailing Hans so he can help them with Hamburg Job.	Chat with Jack on Hans Murschenhofer's Facebook. Warrant for Facebook account access was acquired on 10/03/2017.
29/11/2016	Katie emailed Wang to secure the deal that Daniel and Katie were talking about beforehand. Katie and Wang discussed and made an agreement of the shipment.	Email between Katie and Wang and Daniel to Katie email.
3/12/2016	Daniel was caught on the Gatwick airport with fake passport when one of the customs official saw him from a documentary.	

11. RESULTS

11.1 Pertinent Application Summary

11.1.1 Application 6 Summary – NKHOD Travel <PDF File>

This was a password protected file. This was initially ran through PTRK, but however a number of failed attempts. I decided to search for the password. I ended up looking for it in the receipt booking ticket for Daniel as a comment, "<!--might help open the flight booking... Zxs*9uess8&^dUuG*HMHb@3-->." I typed this in and found a confirmation ticket of all the details for Jack Ascroft of when he was going to Hamburg. In addition, when I was given access to the Facebook, a meeting point in Hamburg suggested that he was going to go to Hamburg in the first place.

11.1.2 Application 6 Summary – SE Report <PDF File>

This was a password protected file again. I found this file with a link with Daniel to Hacker as he mentioned that the password was the last thing Hans did on his Facebook. I did a quick search for Hans on Facebook and it revealed that the password was Einkaufen. I typed this in and an image appeared that was empty. Therefore, I changed the first few bits to 25 50 44 46, and changed the extension to PDF and found a document that revealed the details to Han's Facebook. It contained his username and password.

11.2 Pertinent Email Summary

Daniel to Hacker.eml (Email) was found under "*MyBlog*" under "*Blog*". To retrieve this email, you can double click it by connecting Outlook to view the email. Or, you can highlight the text by bookmarking it in Encase and then changing the format of the text and the email can be displayed. This email highlighted Miko, the Hacker, and Daniel trying to get information on Hans Murschenhofer. Daniel contacted the Hacker to get information and in exchange, they used bitcoin to transfer the money over. They got child pornography images that has been found and a SE Report that has been recovered.

Katie to Wang (Email) , it was encrypted. Therefore, I had to use a numerous of tools to find the password. I used OpenPuff to find a hidden message within XKCD364 folder within Comms. I found an image that had the hidden text file for a public key and private key. In addition, I unlocked this using the password on the image. Once this was unlocked, I used Kleopatra software to decrypt the image. There is a password for decrypting the email, which I used "Passphrase" as written next to it and it decrypted the message to Katie to Wang. It came with an attached image. Therefore, I did used Base64 converter to image and found the attached image.