Forensic Technology in Financial Investigations

DC William Fredrick
Lt. Jon Powers
Det. Scott Donlan
Intro

Deputy Chief of Detectives Bill Fredrick
Department of Law and Public Safety

Attorney General
One of 24 cabinet level positions in NJ State Government
Attorneys and investigators working together

Handle all criminal Prosecutions brought to court by the State of New Jersey

Fed work by other Divisions in the Department of Law and Public Safety
New Jersey Division of Criminal Justice

- Corruption & Government Crime
- Gangs & Organized Crime
- Specialized Crimes
- Financial and Computer Crimes

Four Investigative Bureaus
• Primary Responsibility is the Oversight of Investigative Staff

• Three Financial Squads
  • Whippany
  • Trenton
  • Cherry Hill

• Computer Squad
  • Investigative and Forensic Lab
Simple Facts of Computer Crime

- Many Computer Criminals know less about computers than you do
- They use readily available tools, software and hardware
- They have learned a system to defraud others and stick to that system
- You can investigate much of their activities with free publicly available tools
Simple Facts of Computer Crime

- 85% of critical computerized infrastructure is privately owned.

- The internet connects all people regardless of their intent or usage of the Web.

- Everyone is a neighbor, bankers, muggers, shoppers, designers, con-artists, lovers, scammers, Wall St. traders etc.
Computer Forensics

- Is the analysis of data processing equipment with the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to rebuilding of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer procedure. Analysts determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose. (e.g. typically a home computer, laptop, server, or office workstation)

- COLLECTION, ANALYSIS AND REPORT OF DIGITAL INFORMATION
Deletion

- **Deletion**
  - Is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except using special data recovery tools designed to recover deleted data. Deletion occurs in several levels on modern computer systems.

- **Deleted Data**
  - Is data that, in the past, existed on the computer as live data and which have been deleted by the computer system or user. Although, the data still remains on the hard drive unless the hard drive has been completely wiped. Even after the data itself has been wiped, files or folders may remain on the computer that used to direct to the no longer existing data.

- **Deleted Files**
  - Files, which may have been deleted by the computer user or operating system. Normally deleted files are not removed from the hard drive. The deletion process only alters a directory entry in most cases. This leaves deleted files accessible to forensic examinations.
Internet Protocol

- **IP Address (IPV4 or IPV6)**
  - Internet Protocol Address. It is a series of one- to three-digit numbers separated by periods. It is used to identify a computer connected to the Internet. For example, 212.6.125.76 is an IP address.

- **Internet Service Provider (ISP)**
  - Is a company that provides access to their web site and or access to the Internet. The service provider gives you a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. Newsgroups can also be accessed through this service.
Data about Data

- **HASH** - the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter key than to find it using the original value. It is a digital fingerprint.

- **MetaData**
  - Is contained inside of a file and is not normally visible to the user, but can contain detailed information about the file. Metadata describes the attributes of data - document, data set, database, image, artifact, collection, etc.; A metadata record can include representations of the content, context, structure, quality, condition, and other characteristics for the purposes of representing the data to a potential user - for discovery, access, transfer, and citation.
  - Is information about a particular data set that may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified, and how it is formatted. Users can easily see some metadata, such as file dates and sizes. Other metadata can be hidden or embedded and therefore unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed. (Typically referred to by the less informative shorthand phrase “data about data,” it describes the content, quality, condition, history, and other characteristics of the data.)
Hard Drive Storage

- Unallocated Space
  - Also referred to as free space. This is the area of the hard drive that is free to be written to again. When files are deleted using conventional DOS or Windows commands or are automatically deleted by programs such as word processing applications, the data associated with the file is not actually deleted. The computer simply makes the space available for new files. The old data remains behind on the computer hard drive or floppy diskette to be eventually overwritten with data from new files. This area will also contain file slack that was previously associated with the file.
Networks

- VPN (Virtual Private Network)
  - A private network that utilizes a public telecommunication infrastructure. A VPN uses “tunneling” to encrypt all information ensuring the network remains private and secure.
**Types of Web**

- **Surface - Commercial -** [amazon.com](http://amazon.com) etc
  - The part of the World Wide Web that is accessed openly through browsers.

- **Deep- Specialty - SWIFT / CJIS**
  - the part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks.

- **Dark- TOR etc**
  - the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.
How devices connect to the internet

- **Hard line – Ethernet**
- **Wireless - Home router**
- **Public WiFi**
  - USED TO ANONYMIZE INTERNET USAGE
Memory Trigger #1

- Emails Suspected to be fraudulent
  - Pull the header
  - What can you find in there
  - Follow up on the email address
Trace the email

- Follow IP addresses
  - include in your referral
- Possibly indicates a hosted website
  - Research via online tools
- Discover new email
  - After forensic exam of seized devices
Email Header Example
Info about research tools

CentralOps.net - Advanced online Internet utilities

Domain Dossier
Investigate domains and IP addresses

domain or IP address: 68.232.205.206

- domain whois record
- DNS records
- network whois record
- service scan

user: anonymous [160.93.148.102]
balance: 49 units
log in | account info

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name: mta3.e.lowes.com.
aliases:
addresses: 68.232.205.206

Domain Whois record
Queried whois.internic.net with "dom lowes.com"...
Researching an IP address

- Centralops.net, Arin etc.
- Interpret the return
  - Include found URLs
- Follow up on the info
  - Subpoenas to service providers, web hosting etc.
Social media investigations

- Easily obtainable target information available through social media
- Understanding behavior drives these investigations
- Many criminals refuse to believe law enforcement is looking for them
- Wary criminals still leave evidence behind
Basic Forensic Methods

 DET Scott Donlan
Memory Trigger #2

- Assume everyone uses a smart phone
  - Banking Apps
  - Host of information gained from extraction
    - Chats
    - GPS location
    - Meta Data
    - Can refute alibi
Cell Phone Forensics

- **Hardware**
  - Laptop or Tablet
  - Various vendors
  - Multiple methods

- **Overview of Process**
  - Seize
  - Extract
  - Analyze
  - Report
Cell Phone Forensics - Photo location
Cell Phone Forensics - Chats

Conversation (SMS Message)

Participants (1)
Mom +16092135805

Conversation
- Select/Deselect all 197 messages

From: Mom
Maybe
3/29/2017 08:23 (UTC-05:00)

From: Mom
Whaaa??
3/29/2017 08:23 (UTC-05:00)

To: Mom
Could you go in the bathroom, and find my contact lens boxes. Take out the sets from both, and take pictures of them? I need the prescriptions because vis and I are about to get glasses.
3/29/2017 01:30 (UTC-05:00)

To: Mom
Make sure you specify which is left and right!!
Phone Backups

- Destroyed phones may still yield evidence
  - Cloud Backups
  - Cell Service Carrier
  - SIM card / SD storage
Contacting Providers
http://www.search.org/resources/isp-list/
http://www.search.org/resources/isp-list/
Computer Forensics

- Justifying a Search Warrant on Digital Devices

- Must meet one of three criteria
  - Computer Holds Evidence
  - Used to Facilitate the crime
  - Is a Target of the crime
EnCase Exam Results

Output of Forensic Software
## EVIDENCE (797,230)

<table>
<thead>
<tr>
<th>Item</th>
<th>Type</th>
<th>Category</th>
<th>Date and time</th>
</tr>
</thead>
<tbody>
<tr>
<td>file://System/Library/Frameworks/Ruby.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/CoreServices/NotificationCenter/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Applications/iTunes.app/Contents/PlugIns/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/PrivateFrameworks/Calendar...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Input%20Methods/PressAndHold...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Documentation/Applications/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Library/Widgets/World%20Clock/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Messages/PlugIns/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Applications/Utilities/Grapher.app/Contents/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/PrivateFrameworks/CoreChime...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/Ruby.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/Ruby.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>1/11/2017 10:28:18 PM</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Extensions/ICURDFamily/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/AppKit.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Users/sf/Contents/ Leben/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Users/sf/Contents/ leben/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Applications/Utilities/AirPort%20Utility.app/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/QCAX6.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/QuickTime/QuickTimeFreeWare...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Extensions/ICUIFamily/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/AppKit.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/PrivateFrameworks/CoreWLA...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://Applications/Utilities/System%20Information...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/Frameworks/Ruby.framework/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>file://System/Library/CoreServices/AdOpPrint.app/Resources/...</td>
<td>Safari History</td>
<td>Web Related</td>
<td></td>
</tr>
</tbody>
</table>

**EVIDENCE INFORMATION**

- **Source**: 2018-06-07_09-04-48.E01 - Partition Z (Apple HFS+, 697,84 GB) Macintosh HD (Unallocated Clusters)
- **Location**: Physical Sector 147205964
- **Evidence number**: 2018-06-07_09-04-48.E01

**DETAILS**

- **Title**: Yah

---

**WEB RELATED**: 540,909

**CHAT**: 531

**MEDIA**: 232,271

**EMAIL**: 135

**DOCUMENTS**: 5,498

**PEER TO PEER**: 9,846

**OPERATING SYSTEM**: 4
Forensic Software Summary View

CASE OVERVIEW

CASE SUMMARY NOTES
Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: K.Madore
Case summary:

CASE PROCESSING DETAILS

CASE NUMBER: 2018-02516
SCAN 1
Scan by: K.Madore
Scan date: 6/9/2018 12:33:23 AM
Scan description: 750GB ToshibaHDD_SN136CCBT
Taken from Apple laptop

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

OPEN CASE INFORMATION FILE

The AEXM/examine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

OPEN LOG FILE

EVIDENCE OVERVIEW

Evidence number: 2018-06-07_09-04-48.001 (797,230)
Description:
Location: 2018-06-07_09-04-48.001
Platform: Computer
No picture added

PLACES TO START

TOP ARTIFACT CATEGORIES

VIEW ALL ARTIFACT CATEGORIES

Evidence source: All
Number of artifacts: 797,230
Web Related:
Media: 232,271
Peer to Peer:
Retained Results:
Documents:
Chat:
Email:

TAGS AND COMMENTS

KEYWORD MATCHES

No keyword matches were found while processing the case. Either no keyword list was provided, or there were no matches in the specified list.
IMPORT KEYWORD LIST

PASSWORDS AND TOKENS

No cloud passwords or tokens were found while processing the case.

PROFILES

Use profiles to associate identifiers (like user names, email addresses, phone numbers, and more) with a specific person.
MANAGE PROFILES

MILITARY CATEGORIZATION (97,256)

VIEW ALL MILITARY CATEGORIZATION MATCHES

CATEGORY | MATCHES
--- | ---
2 | 51,516
0 | 38,022
1 | 7,712
3 | 6
Alibi “It was my room mate”

- User profile

- Putting the man behind the keyboard
  - Timeline analysis
  - Password protected logins
  - Simultaneous logins
Video Forensics

- Interesting evidence found
  - Forensic exam of ATM video
    - Disguised person holds car keys
      - Gym member ID tag on key ring
    - Disguised Person with noticeable limp
    - Hooded person with unique ring
Memory Trigger #3

- The had to pay for services and get paid out too
- Prepaid Cards- Green Dot // Vanilla
Bitcoin

- Peer to Peer exchange
  - Basement Bitcoin miners need cash
- Point of Control
  - FINCEN regulations
  - Coinbank.com online clearing house
Cryptocurrency (Bitcoin)

- **Web-based Wallets**: xapo, GreenAddress, coinbase
- **Hardware Wallets**: Trezor
- **Mobile Wallets**: Gopay
- **Desktop Wallets**: Armory
- **Paper Wallet (Cold Storage)**: Electrum

**Wallets**
Cryptocurrency (Bitcoin)

https://coinatmradar.com/

**Bitcoin ATM map.**

*Use our map to find bitcoin or other cryptocurrency ATM locations as well as various alternative crypto-cash exchange services.*

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3236</strong></td>
<td><strong>41178</strong></td>
<td><strong>70</strong></td>
<td><strong>31</strong></td>
<td><strong>446</strong></td>
</tr>
<tr>
<td>Bitcoin ATMs</td>
<td>Other services</td>
<td>Countries</td>
<td>Producers</td>
<td>Operators</td>
</tr>
</tbody>
</table>

Know of a bitcoin ATM missing on the map? Submit required details.
Cryptocurrency (Bitcoin)
Cryptocurrency (Bitcoin)

Technically it isn’t an ATM, it’s a Kiosk.

Bitcoin Kiosk operators, defined by FinCEN, are “exchangers” and therefore considered Money Service Businesses (MSBs), or specifically, *money transmitters*.

- Per FinCEN, a *money transmitter* is defined as:
  “a person that provides money transmission services,
or any other person engaged in the transfer of funds”.

FinCEN does not differentiate between real currencies and virtual convertible currencies (FIN-2013-G001).

- As a money transmitters they are subject to Bank Secrecy Act (BSA) regulations per FinCEN.

As a result of this determination Kiosk operators:

1. Must typically register as an MSB,
2. Must implement a BSA and anti-money laundering (AML) program
Tor and the Dark Web

7,900,000,000,000,000,000,000
1,000,000,000,000 = 1 Terabyte
The “dark web” is similarly made up of sites that are not indexed by search engines. However, websites on the dark web are also anonymously-hosted and are only accessible with special software and browsers that mask one's IP address. The most common tool to navigate the dark web is the Tor (The Onion Router) browser. Tor routes internet traffic through a series of “nodes,” which are computers hosted on the Tor network by volunteers. The process of randomly bouncing data through many different nodes makes it nearly impossible to trace the data back to an internet user. In fact, the U.S. Naval Research Laboratory initially developed Tor as a way to secure communications.
Tor and the Dark Web

Tor client -> Entry guard

Tor network:
- Middle relay
- Exit relay

Destination

Encrypted by Tor
Not encrypted by Tor
Tor and the Dark Web

USfakeIDs

US Fake Drivers Licenses - Scannable, Holograms, UV etc

Our fake drivers licenses are all scannable, contain original hologram and UV, microprint, laser engraving etc. Shipping from the US within 48 hours! We only sell the best quality, you will not find better IDs anywhere.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Buy now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delaware</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>Illinois</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>South Carolina</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>New Jersey</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>Colorado</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>200 USD = 0.029 $</td>
<td>1</td>
<td>X</td>
</tr>
</tbody>
</table>
Tor and the Dark Web

Cash Machine™ For Everybody!
Best Solution to get Money Quickly

- Fresh and New Accounts Every Day!
- Different Balances and Prices Available
- All our Goods are 100% Verified
- Free & Clean socks5 for each account (in the same Town as the Holder)
- All Accounts have the Balance Mentioned and are Linked to Bank Account and Credit Card of the owner
- Account Replacing If Amount is Different than what We've Agreed
- Complete Step by Step Walkthrough Guide (Very Easy Cash Out!)
- Cashing Out WORLDWIDE in Less Than 4 Hours

What do you need?

- Wells Fargo Bank Account / min4
- Email (You will receive every order by email)

Buy now!
Tor and the Dark Web
Tor and the Dark Web

These cards work in ALL Countries around the globe, Enjoy!

Visa Prepaid Cards
At BITCARDS, we offer a variety of Visa Prepaid Cards. These cards have all the benefits you would expect from Visa and are simple and convenient to use – even if you do not have a bank account or an established banking history.

Prepaid Visa Classic
- Balance: Between $2560 and $2800
- Withdrawal Limit: $100/day

Prepaid Visa Gold
- Balance: Between $3500 and $4000
- Withdrawal Limit: $250/day

Prepaid Visa Platinum
- Balance: Between $13000 and $15000
- Withdrawal Limit: $800/day

Prepaid Visa Infinite
- Balance: Between $10000 and $12000
- Withdrawal Limit: $2000/day

American Express Cards

American Express Business Blue
- Balance: Between $23000 and $25000
- Withdrawal Limit: $1200/day

American Express Business Gold
- Balance: Between $75000 and $80000
- Withdrawal Limit: $2500/day

American Express Business Platinum
- Balance: Between $100000 and $110000
- Withdrawal Limit: $5000/day

Please Note: Balances and Withdrawal Limits are per card.
### Tor and the Dark Web

#### The Green Machine

<table>
<thead>
<tr>
<th>Title</th>
<th>User</th>
<th>Last post</th>
<th>Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big sale!</td>
<td>mrfungi</td>
<td>100 days 10 hours ago by mrfungi</td>
<td>9</td>
</tr>
<tr>
<td>Looking for supplier of tadalafil</td>
<td>tadalafil</td>
<td>109 days 3 hours ago by tadalafil</td>
<td>1</td>
</tr>
<tr>
<td>AMATEUR</td>
<td>lecrepa</td>
<td>109 days 3 hours ago by lecrepa</td>
<td>1</td>
</tr>
<tr>
<td>I need Fixed Matches Seller. No Scams</td>
<td>Bomboobie</td>
<td>109 days 3 hours ago by mikey</td>
<td>2</td>
</tr>
<tr>
<td>Cloned Cards FAQ - READ BEFORE ORDERING!!</td>
<td>mrfungi</td>
<td>110 days 5 hours ago by mrfungi</td>
<td>43</td>
</tr>
<tr>
<td>Back online!</td>
<td>admin</td>
<td>110 days 10 hours ago by admin</td>
<td>2</td>
</tr>
<tr>
<td>Christmas sale!</td>
<td>mrfungi</td>
<td>117 days 12 hours ago by pulsar</td>
<td>6</td>
</tr>
<tr>
<td>CLONED CREDIT CARDS! - Real cards with stolen info</td>
<td>mrfungi</td>
<td>302 days 9 hours ago by satoshibox</td>
<td>266</td>
</tr>
<tr>
<td>Here I have Very Deep Data Gaining Directly From</td>
<td>satoshibox</td>
<td>302 days 9 hours ago by satoshibox</td>
<td>2</td>
</tr>
<tr>
<td>5 cc Cloned International with Personal Data</td>
<td>pdiesel6074</td>
<td>396 days 17 hours ago by pdiesel6074</td>
<td>1</td>
</tr>
<tr>
<td>If you are using tor2mail, please read this</td>
<td>mrfungi</td>
<td>396 days 20 hours ago by mrfungi</td>
<td>1</td>
</tr>
<tr>
<td>Need to transfer from check account to cash</td>
<td>lowelyf</td>
<td>401 days 4 hours ago by lowelyf</td>
<td>1</td>
</tr>
<tr>
<td>Looking for someone to work with, selling cards</td>
<td>wizzkiller44</td>
<td>401 days 6 hours ago by wizzkiller44</td>
<td>1</td>
</tr>
<tr>
<td>BITCOIN FREE</td>
<td>durO14</td>
<td>401 days 11 hours ago by amatterasau</td>
<td>4</td>
</tr>
<tr>
<td>$75 for $500 card</td>
<td>travisscott</td>
<td>401 days 12 hours ago by mrfungi</td>
<td>3</td>
</tr>
<tr>
<td>Plenty of fresh accounts!</td>
<td>PayedPals</td>
<td>401 days 16 hours ago by keksas</td>
<td>199</td>
</tr>
<tr>
<td>how to hack facebook?</td>
<td>Ghost89</td>
<td>401 days 18 hours ago by Raj86</td>
<td>3</td>
</tr>
<tr>
<td>hi</td>
<td>broker</td>
<td>402 days 5 hours ago by broker</td>
<td>3</td>
</tr>
<tr>
<td>US INFO FOR SALE</td>
<td>XMISTERP</td>
<td>402 days 6 hours ago by XMISTERP</td>
<td>1</td>
</tr>
<tr>
<td>new user</td>
<td>Arcad</td>
<td>402 days 7 hours ago by Arcad</td>
<td>3</td>
</tr>
<tr>
<td>part supplies</td>
<td>dutchmaster</td>
<td>402 days 7 hours ago by dutchmaster</td>
<td>1</td>
</tr>
<tr>
<td>Fake cocaine for sale</td>
<td>kingbull</td>
<td>402 days 9 hours ago by kingbull</td>
<td>6</td>
</tr>
</tbody>
</table>
Hello everyone!

I have gathered the equipment for cloning CC's, learned and perfected my method, and now I'm ready to start sharing these wonderful cards with my deep web friends.

To make sure we all understand, these are REAL CARDS mailed to you. I use my mag strip writer to write stolen CC data to the cards. They can be used anywhere, in any store, just swipe and go. They are printed to look just like real VISA cards, and contain the data from VISA Signature cards with $5000 limits.

Price is $100 per card.  
I will emboss the cards with any name you wish.  
Guaranteed to have at least $3000 left on CC limit, most are over $4000.

Want several? I will give a great deal on orders of more than 1 card. Order 2 save 10%, order 5 save 25%, order 10 save 35%!!!

Cards are discreetly mailed worldwide using priority mail, with tracking numbers. Upgrade to express shipping for an additional $15.

Same day shipping in most cases!

Mrfungi2013@hushmail.com
Tor and the Dark Web

**$ The Green Machine $$**

Plenty of fresh accounts!

Return to board index

You are not logged in. Log in | Sign up

--PayedPals posted 1904 days 7 hours ago:

Guys I have a ton of fresh accounts. Balances from $733 up to $5872. Price is 10% as always.

EMAIL ME
PayedPals@tormail.org

--PayedPals posted 1904 days 6 hours ago:

Bitcoins, Greendot Moneypaks, Western Union, and Liberty Reserve accepted.

--merlin posted 1904 days 3 hours ago:

Bought one with $1100 bout an hour ago. He's a straight up dude, shit's legit. tutorial is awesome, simple genius. I'm hooked!

--zbidox posted 1904 days 0 hours ago:

please send me a paypal account (just one) please because I'm poor and I want even if it is for a belief to buy something on the internet, if it is possible I ask you contact me on zikassestyel@yahoo.fr

--LinkBR posted 1903 days 22 hours ago:

PayPal Send money to my account please: clarinbah2010@hotmail.com
Working together on AML Cases

- Referral contents
- Cooperative actions
  - Pretense meetings
  - Sting Operations
  - AML-Task Force
- Forensics and Digital evidence
  - Expand Scope of Investigation
  - Provides Evidence of criminal activity
  - Establish ability, intent to commit crime
Case Scenario Begins

- Financial Crime of some sort
  - Digital in nature
  - Money Laundering- structuring, tax evasion
  - BSA activity
  - Quarterly audit

- Do Banks refer only after Bank has been victimized?
- Are there policies in place for coop investigations?
Search Warrant Criteria

- Purpose is to preserve evidence of a crime while safeguarding the process of a prosecution and legal rights defendant.
- Must be adequately specific about:
  - the probable cause to justify a search
  - the place or premises to be searched
  - the items or property to be seized
Case Study One

- Fraudulent Loan Ring
  - Secure a loan in false identity
  - Accept Half in cash
  - Disappear

- DCJ and Bank Proactively Look Forward
  - Arrange in person closing
  - Target shows ID
  - Accepts cash
  - Arrest made as Target and Driver prepare to leave
Case Study Two

- Spoofed Email
  - Assumed identity of vendor
  - Socially engineered attack

- Investigative Actions
  - Email header info
  - Trace route
    - 75 linked domains
  - Domain Info
    - Stolen Credit Card
Case Work Summary

- Follow BSA requirements
- Keep in mind money trail and digital trail
- Identify moments of positive ID
  - ATM cameras
  - Physical signatures
  - Bank Surveillance
CONTACTS

Anti-Money Laundering Task Force
AMLTaskForce@njdcj.org
609-376-2500

LT Lisa Shea
25 market St
Trenton NJ
609-376-2385

DCJ Cybercrime Unit
1200 Negron Dr.
Hamilton NJ
609-584-5051

DET Scott Donlan
Ext 5638

LT Jon Powers
Ext. 5601