

## Identifying Fraudulent Electronic Returns & Blocking Refunds

Penny Feneis & Stacy Lessard  
Minnesota Department of Revenue, Individual Income Tax

## What we look for

- Fraudulent income tax refund claims
  - Invalid wages, withholding, and other refundable credit claims
  - EIC equivalent
- Collaborate on investigations with IRS CID as well as our counterparts in other states through our Suspicious Filer User Group



## How is a Fraudulent Tax Return Filed?

- Electronically
  - H&R Block, Liberty Tax Service, etc.
    - Local offices
- Over the Internet
  - Boxed software (HRB TaxCut, TurboTax, etc.)
  - Web sites
    - [www.turbotax.com](http://www.turbotax.com)
    - [www.HRBlock.com](http://www.HRBlock.com)
    - [www.TaxSlayer.com](http://www.TaxSlayer.com)
    - [www.LibertyTax.com](http://www.LibertyTax.com)
- Paper
  - Forms filled out by hand and mailed in

## Why does the electronic age make things difficult?

TAXSLAYER.COM

Need help? Type your question here... Search

Register

**New to TaxSlayer.com ?**

Create a Username:   
(Must be 4-20 characters.)

Create a Password:   
Re-Enter Password:   
(Password is case-sensitive.)

Current Email Address:   
Re-Enter Email:   
(Note: Email must be valid.)

Select a security question:   
Please enter the answer:

I wish to upgrade this account to the Premium Version. [Listed Here](#)

I agree to the Terms and Conditions [Listed Here](#)

I agree to the Terms of IRS Section 7216 [Listed Here](#)

**Start Now**

**Already a TaxSlayer.com User ?**

**Secure Sign In**

- Continue Return
- Check Status
- Print Return
- Account Info
- Re-Download
- Print Prior Year

**Important**

ALL email correspondence will be sent from this address:  
support@taxslayer.com

**Return To Home Page**

©2008 TaxSlayer.com cannot guarantee date of receipt of refund.

How much of this is real?  
**NONE!**

## How much is real?

- Only the IP Address that the return is transmitted from is real, all else is created
- So you must be able to capture or subpoena the IPA (Internet Protocol Address)
- IPA can be static or dynamic
  - Static – fixed, as in you own it (schools, government, big business)
  - Dynamic – assigned from IPA pool (AOL, NetZero, Yahoo, etc.)
  - 68.102.240.180 (sample)
  - 217.21.114.115 (foreign sample)

## Who-is Websites

- **ARIN – American Registry for Internet Numbers**
  - <http://www.arin.net/whois/>
- **AfriNIC – African Network Information Centre**
  - <http://www.afrinic.net/cgi-bin/whois>
- **APNIC – Asia Pacific Network Information Centre**
  - <http://www.apnic.net/search/index.html>
- **LACNIC – Latin American and Caribbean Internet Addresses Registry**
  - <http://lacnic.net/cgi-bin/lacnic/whois>
- **RIPE – Réseaux IP Européens**
  - <http://www.ripe.net/perl/whois/>
- **InterNIC – Internet Domain Name Registration Services, U.S. Dept of Commerce**
  - <http://www.internic.net/whois.html>



# ARIN Website

ARIN: WHOIS Database Search - Department of Revenue Services

File Edit View Favorites Tools Help

Back Search Favorites

Address <http://www.arin.net/whois/>

## ARIN WHOIS Database Search

Search ARIN WHOIS for:

Need Help?

ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system (AS) numbers, organizations or customers that are associated with these resources, and related Points of Contact (POC).

ARIN's WHOIS will NOT locate any domain related information, nor any information relating to military networks. Please use whois.internic.net to locate domain information, and whois.nic.mil for military network information.

Many operating systems provide a whois utility. To conduct a query from the command line, the format is:

```
whois -h hostname identifier e.g. whois -h whois.arin.net
```

To obtain a more specific response, you may conduct a search by using certain flags. Many of these flags can be combined to tailor the desired output. Flags must be separated from each other and from the search term by a space. Your results will vary depending on the refinements you apply in your search. Listed below are the flags currently available; you may only use one flag from each flag-type in a query (i.e. one record type, one attribute, etc).

### Relevant Links

- [ARIN Home Page](#)
- [ARIN Site Map](#)
- [Request Bulk Copies of ARIN WHOIS Data](#)
- [Training](#)

*Querying ARIN's WHOIS*

An online training module to learn to structure a query in ARIN's WHOIS and how to understand the information that is retrieved.

# ARIN Search Results

Address <http://ws.arin.net/whois/>

## ARIN WHOIS Database Search

Relevant Links: [ARIN Home Page](#) [ARIN Site Map](#) Training: [Querying ARIN's WHOIS](#)

Search ARIN WHOIS for: **68.102.240.180**

**ISP – Internet Service Provider**

Cox Communications Inc. NETBLK-WI-RDC-68-102-0-0 (**NET-68-102-0-0-1**)  
68.102.0.0 - 68.103.255.255

Cox Communications Inc. COX-ATLANTA-2 (**NET-68-96-0-0-1**)  
68.96.0.0 - 68.111.255.255

# ARIN WHOIS database, last updated 2008-02-18 19:10  
# Enter ? for additional hints on searching ARIN's WHOIS database.

Other WHOIS Servers: [AfrNIC](#) [APNIC](#) [LACNIC](#) [RIPE](#) [InterNIC](#)

[Request Bulk Copies of ARIN WHOIS Data](#)

Copyright © 1997-2007 American Registry for Internet Numbers. All Rights Reserved.

# Now what?

Address <http://ws.arin.net/whois/?queryinput=%20NET-68-102-0-0-1>

## ARIN WHOIS Database Search

Relevant Links: [ARIN Home Page](#) [ARIN Site Map](#) Training: [Querying ARIN's WHOIS](#)

Search ARIN WHOIS for: ! NET-68-102-0-0-1

Submit Query

OrgName: Cox Communications Inc.  
OrgID: CXA  
Address: 1400 Lake Hearn Drive  
City: Atlanta  
StateProv: GA  
PostalCode: 30313  
Country: US

Issue a subpoena  
to ISP for customer info

NetRange: 68.102.0.0 - 68.103.255.255  
CIDR: 68.102.0.0/15  
NetName: NETLK-WI-RDC-68-102-0-0  
NetHandle: NET-68-102-0-0-1  
Parent: NET-68-96-0-0-1  
NetType: ~~Designated~~

Comment: For legal requests/assistance please use the following contact information:  
Comment:  
Comment: Cox Subpoena Phone: 404-269-0100  
Comment:  
Comment: Cox Subpoena Info: <http://www.cox.com/policy/learninformation/default.asp>  
RegDate: 2002-05-15  
Updated: 2007-08-16

OrgAbuseHandle: IC146-ARIN  
OrgAbuseName: Cox Communications, Inc  
OrgAbusePhone: +1-404-269-7626  
OrgAbuseEmail: abuse@cox.net

# KENYAN TAX FRAUD



**ID Theft**

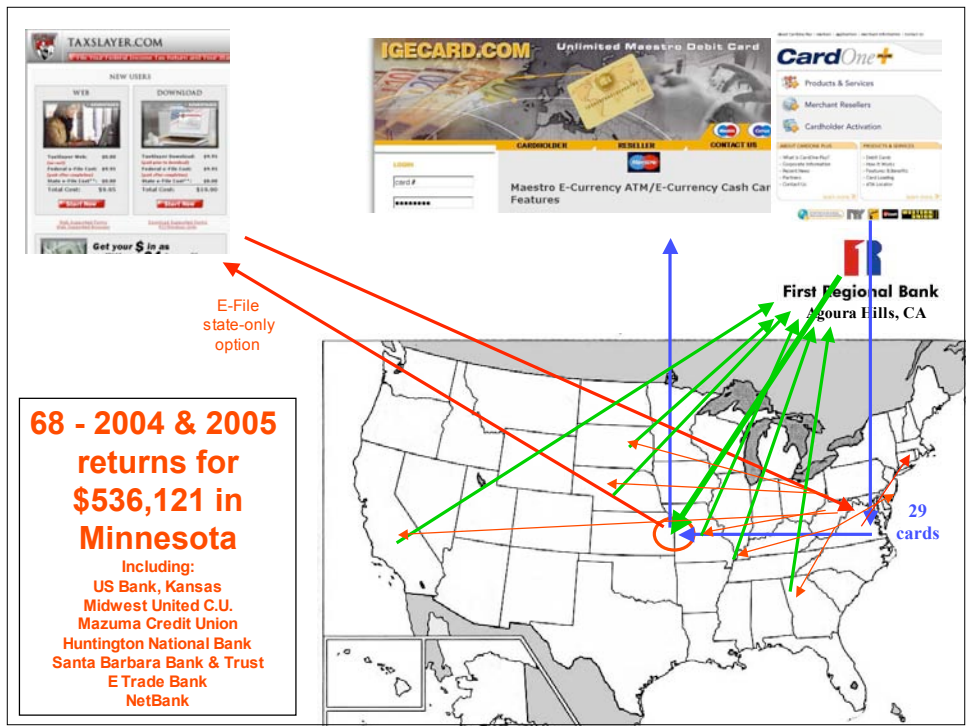
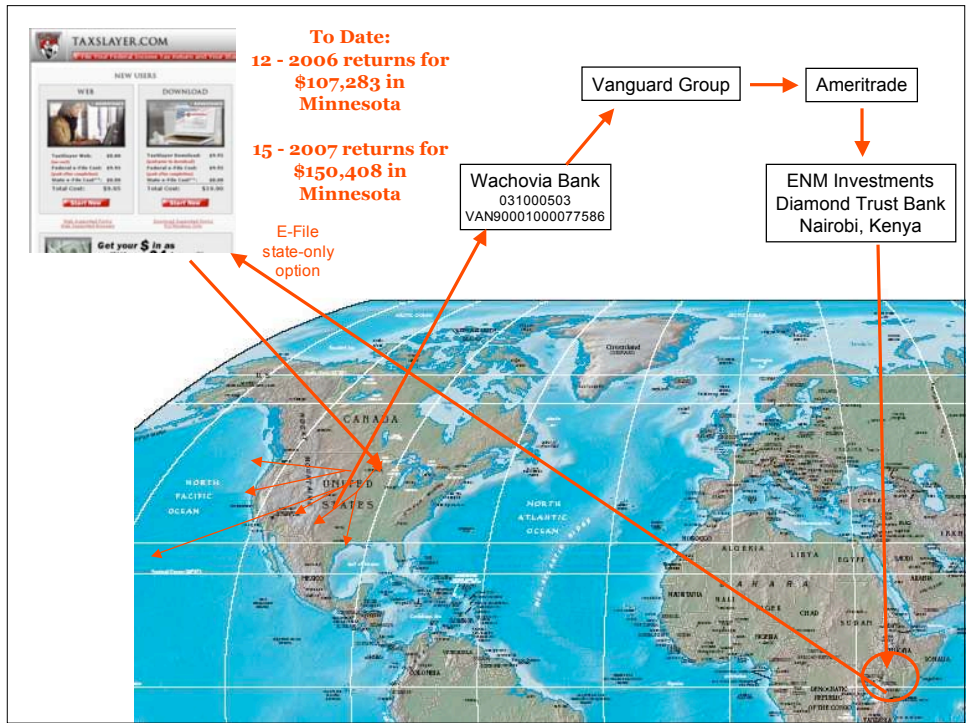
**Kenya**



**Tax Returns**

**Refunds  
Deposited**

**Cash  
Withdrawn**



## The “Kansas/Kenya” Gang



**\$793,812**  
= **95 returns**  
in Minnesota

## Essential Steps for Blocking E-File

- Block SSNs
- Block Addresses
- Block Bank Accounts
- Change state disclosure laws (if needed)
  - A victim state should be able to disclose fraud info to any government agency or government employee
- Share alerts with other states
- Coordinate investigations
  - IRS, FBI, Secret Service, Postal Inspectors, State Police, State Tax Agents, local police, INTERPOL

## Share information with other states

The screenshot shows a software interface for managing PGP keys. At the top, there is a menu bar with 'File', 'Edit', 'View', 'Tools', 'Keys', and 'Help'. Below the menu bar are several icons: 'New PGP Zip', 'Verify PGP Zip', 'Shred Files', 'KeySearch', and 'Sync Keys', followed by a 'Find:' search box. On the left side, there is a sidebar with a 'PGP Keys' dropdown menu. Under this menu, there are options for 'All Keys', 'My Private Keys', and 'Search for Keys'. Below these are buttons for 'Email this Recipient' and 'Email this Key'. Further down are sections for 'PGP Messaging', 'PGP Zip', and 'PGP Disk'. The main area is titled 'All Keys' and contains a table with three columns: 'Name', 'Email', and 'Validity'. The table lists 20 entries, each with a checkbox, a key icon, a name, an email address, and a green circle indicating validity.

| Name  | Email                            | Validity |
|---|----------------------------------|----------|
| <input type="checkbox"/> Ann Roe-Lewis          | Ann.Roe-Lewis@ky.gov             | ●        |
| <input type="checkbox"/> Anthony Beccone        | abeccone@state.pa.us             | ●        |
| <input type="checkbox"/> Bob Godin              | godinb@tax.state.ri.us           | ●        |
| <input type="checkbox"/> Cal Mellor             | cal.mellor@po.state.ct.us        | ●        |
| <input type="checkbox"/> Charles Ranaghan       | ranaghanc@dor.state.ma.us        | ●        |
| <input type="checkbox"/> Christina C. Ward      | Christina.C.Ward@Maine.gov       | ●        |
| <input type="checkbox"/> David Smith            | dsmith@oktax.state.ok.us         | ●        |
| <input type="checkbox"/> denise backstrom       | dbackstrom@state.mt.us           | ●        |
| <input type="checkbox"/> Dominic L. Vitale      | dominic.vitale@treas.state.nj.us | ●        |
| <input type="checkbox"/> Dottie Perkins         | dperkins@revenue.state.il.us     | ●        |
| <input type="checkbox"/> Fran Krejci            | fkrejci@rev.state.ne.us          | ●        |
| <input type="checkbox"/> Frederick A. Greenwood | greenwoodf@dor.state.ma.us       | ●        |
| <input type="checkbox"/> Hillary C. Burgher     | hillaryc.burgher@ky.gov          | ●        |
| <input type="checkbox"/> Jackie Bender          | Jacquelin_Bender@tax.state.ny.us | ●        |
| <input type="checkbox"/> James Lucy             | jlucy@revenue.state.al.us        | ●        |
| <input type="checkbox"/> James Stewart          | jastewart@state.de.us            | ●        |
| <input type="checkbox"/> Janet M. Avery         | averyj@dor.state.ma.us           | ●        |
| <input type="checkbox"/> Jane Royston           | jroyston@dor.state.wi.us         | ●        |
| <input type="checkbox"/> Jennifer Johnson       | jjohnson@rev.state.ne.us         | ●        |
| <input type="checkbox"/> Jim Buller             | jbuller@rev.state.ne.us          | ●        |
| <input type="checkbox"/> John Bernasconi        | jbernasconi@tax.idaho.gov        | ●        |
| <input type="checkbox"/> Karen Hamann           | khamann@gatax.org                | ●        |

## Other ideas for blocking E-Fraud

- Exchange program manuals
- Share validation resources
- Solicit new member states
- Monthly Conference calls
- Review trends & techniques at an annual meeting (closed session)

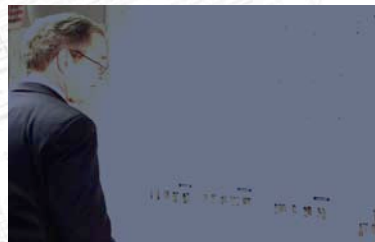


## Past Analysis Methods

- Paper charts: overly time consuming and difficult to edit, disclosure issues
- Excel spreadsheets: difficult to show multiple links between suspects, employers, bank accounts, etc.
- Multiple print-outs: ineffective in storing related data in easy to locate groups

## New Method

- i2 Analyst's Notebook
- i2 Analyst's Notebook is used by over 2,000 organizations worldwide including:
  - IRS - CID
  - FBI
  - Homeland Security
  - state and local law enforcement



President Bush reviewing i2 charts produced at the Financial Crimes Enforcement Network (FINCEN)

## Analysis Criteria

Common data we seek links between:

- Address
- Employer
- Relation
- Bank Account
- Filing Method
- Income Amount
- IP Address
- Preparer



## Analyst's Notebook

### Visualize

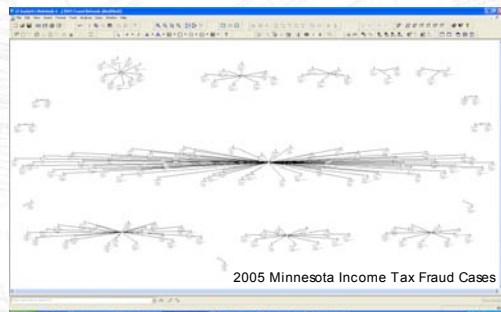
- Create visual timelines
- Expose hidden relationships

### Analyze

- Identify Clusters
- Visual Search or Query
- Locate Paths Between entities
- Find and merge similar entities
- List Items
- Select multiple Chart Layouts
- Change Representation

### Communicate

- Brief Superiors Quickly
- Freely distribute charts



*"i2 software has been used in every major FBI investigation since 1994"*

**Darryl Barton, FBI Retired**

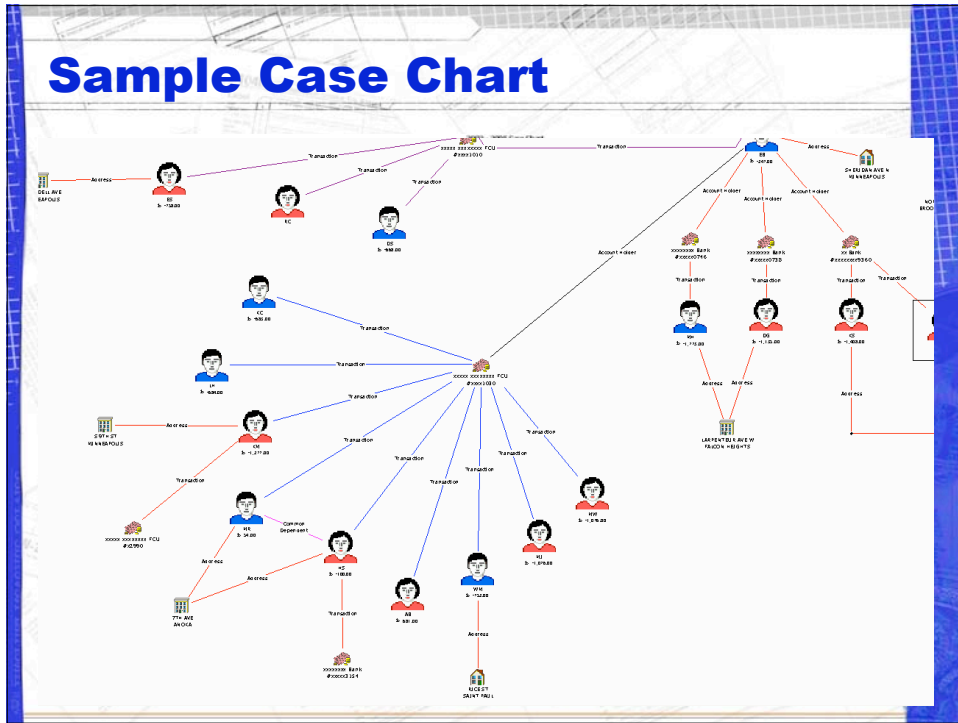
## **Abilities of i2 Analyst Notebook**

- Import data already stored in Excel and manipulate the data to show all links between suspects
- Multiple layouts to present data in the most effective way
- Grade and evaluate data based on the reliability of the source
- Embed pictures, letters, and other records directly accessible from the chart

## **Benefits of i2 Analyst Notebook**

- Protects DOR disclosure practices
- Collect very detailed information and present in a concise manner understandable to multiple persons
- Ability to simplify our referral of cases to our Criminal Division
- Prevent repetition of investigative actions by making information accessible to all DOR employees involved in the investigation

## Sample Case Chart



## Disadvantages

- Each computer must have a separate license.
  - A Chart Reader can be installed on any number of computers free but the Chart Reader does not allow editing capabilities
  - DOR has remedied this issue for us by installing the software & license on a shared laptop, making the program portable and accessible by all fraud investigators
  - Network dongles



## Why bother with all this?

MY SOCIAL SECURITY # IS  
**457-55-5462**

I'm Todd Davis, CEO of LifeLock, and this really is my social security number.\* I'm here just to prove how safe your identity can be with LifeLock. All of us, no matter how careful, can become victims of identity theft. In fact, every three seconds another identity is stolen.

Do you ever worry about identity theft? If so, it's time you got to know LifeLock. We work to stop identity theft before it happens. We're so confident, we back our clients with a \$1 million dollar guarantee. If for any reason you fall victim to identity theft, we will spend up to \$1 million to hire the finest professionals to repair the damage and restore your good name. Period.

Security, peace of mind, protection—that's what LifeLock provides, along with the added bonus of reduced junk mail and pre-approved credit card offers. Normally it's just \$10 a month, but now you can try us free for 30 days. Protect yourself, your family and all you've worked for. Guarantee your good name today.



## Questions?

### Contacts:

Penny Feneis  
Minnesota DOR  
Individual Income Tax  
Fraud Detection  
651-556-6607  
[penny.feneis@state.mn.us](mailto:penny.feneis@state.mn.us)



Stacy Lessard  
Minnesota DOR  
Individual Income Tax  
Fraud Detection  
651-556-6640  
[stacy.lessard@state.mn.us](mailto:stacy.lessard@state.mn.us)