

# ICAC TASK FORCE

## Griffeye Analyze DI - Basics

Presented by:

Jim Cole, Special Agent, HSI

Richard Brown, Technology Advancement Officer, ICMEC

September 26, 2015

# Webinar Information

---

This webinar is supported by grant 2013-MC-FX-K003, provided by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), and is brought to you by the ICAC Training & Technical Assistance Program.

*Points of view or opinions expressed in this webinar are those of the presenter(s) and do not necessarily represent the official position or policies of OJJDP, the U.S. Department of Justice or Fox Valley Technical College.*

ICAC Training & Technical Assistance is a program of the Fox Valley Technical College-National Criminal Justice Training Center (NCJTC).

# During the Webinar

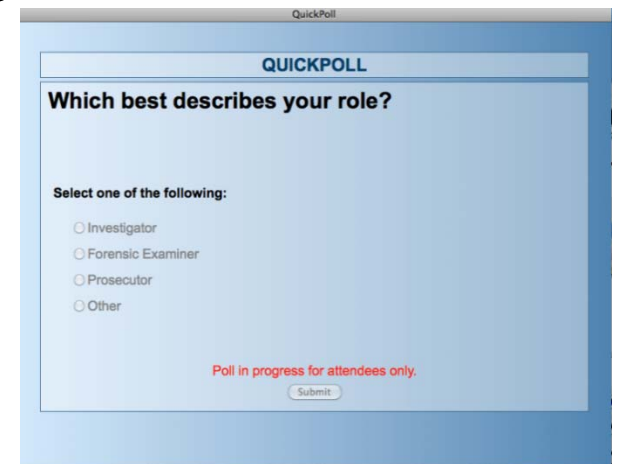
---

- All attendees will be muted.
- If you desire to ask a question, please use the questions section of the GoToWebinar dialogue box, typically on the right side of your screen.
- Please do not raise your hand for questions, we can not unmute you.
- Questions will either be answered directly by a panelist or asked to the presenter who will answer.

# Poll Questions

---

- Poll questions may be asked during the webinar. They are asked so we can better understand the audience and provide the most useful information to you.
- As they will only be open a short period of time, please respond promptly.



QuickPoll

**QUICKPOLL**

**Which best describes your role?**

Select one of the following:

- ☐ Investigator
- ☐ Forensic Examiner
- ☐ Prosecutor
- ☐ Other

Poll in progress for attendees only.

Submit

---

# **Poll Questions 2 thru 4**



# PROJECT VIC



# Why Project VIC

---



No standards for image signatures

No standards for sharing image signatures (hash values)

No quality control

Lack of interoperability

No automation

# Project VIC GOALS

## Standard Image & Video Fingerprints

Microsoft PhotoDNA  
Friend F1

## VICS Hash Set

Quality Controlled  
Database of known  
images and videos.



## A Open Standard to Share Data

VICS Protocol



## Victim Centric Process

Movement toward  
victim focused  
investigations and  
forensics vs offender  
focused

# Project VIC Results

---

## **Increased Efficiency**

HSI Dallas reduced forensic workload from 9 months to 1 week.

## **More Victims Rescued**

Arizona ICAC success in first case after implementing Project VIC

## **Less Exposure**

Increased efficiency means less exposure of harmful material to reviewing investigators



## **Better Convictions**

Enable investigators to find production material early on.

# How Do I Sign Up for Project VIC

---



ICAC COPS has taken over the administration of the Project VIC Registration and distribution of Encryption Certificates

You will also find e-Learning Modules and support forms for Project VIC

# How Do I Sign Up for Project VIC

---



There are two entry ways for Registration:

[accounts.projectvic.org](https://accounts.projectvic.org)

[www.icaccops.com/users](https://www.icaccops.com/users)

# How Do I Sign Up for Project VIC

---



Lets take a look at the first entry point:

[accounts.projectvic.org](https://accounts.projectvic.org)

# accounts.projectvic.org



A screenshot of a web browser window showing the login page for accounts.projectvic.org. The browser's address bar is highlighted in yellow and contains the URL "http://accounts.projectvic.org/login.asp". The browser's title bar reads "ICAC Child Online P". The page features the Project VIC logo in the top left corner. Below the logo is a blue vertical bar with the text "Request An Account" in white. To the right of this bar, the text "Your IP address has been logged: 72.76.111.135" is displayed. Below this, there are input fields for "First Last Name" and "Password", followed by a "Submit" button. At the bottom of the page, the text "Request Account" is visible, along with a copyright notice: "Copyright 2013 ICAC COPS. All Rights Reserved."

Request An Account

Your IP address has been logged:  
72.76.111.135

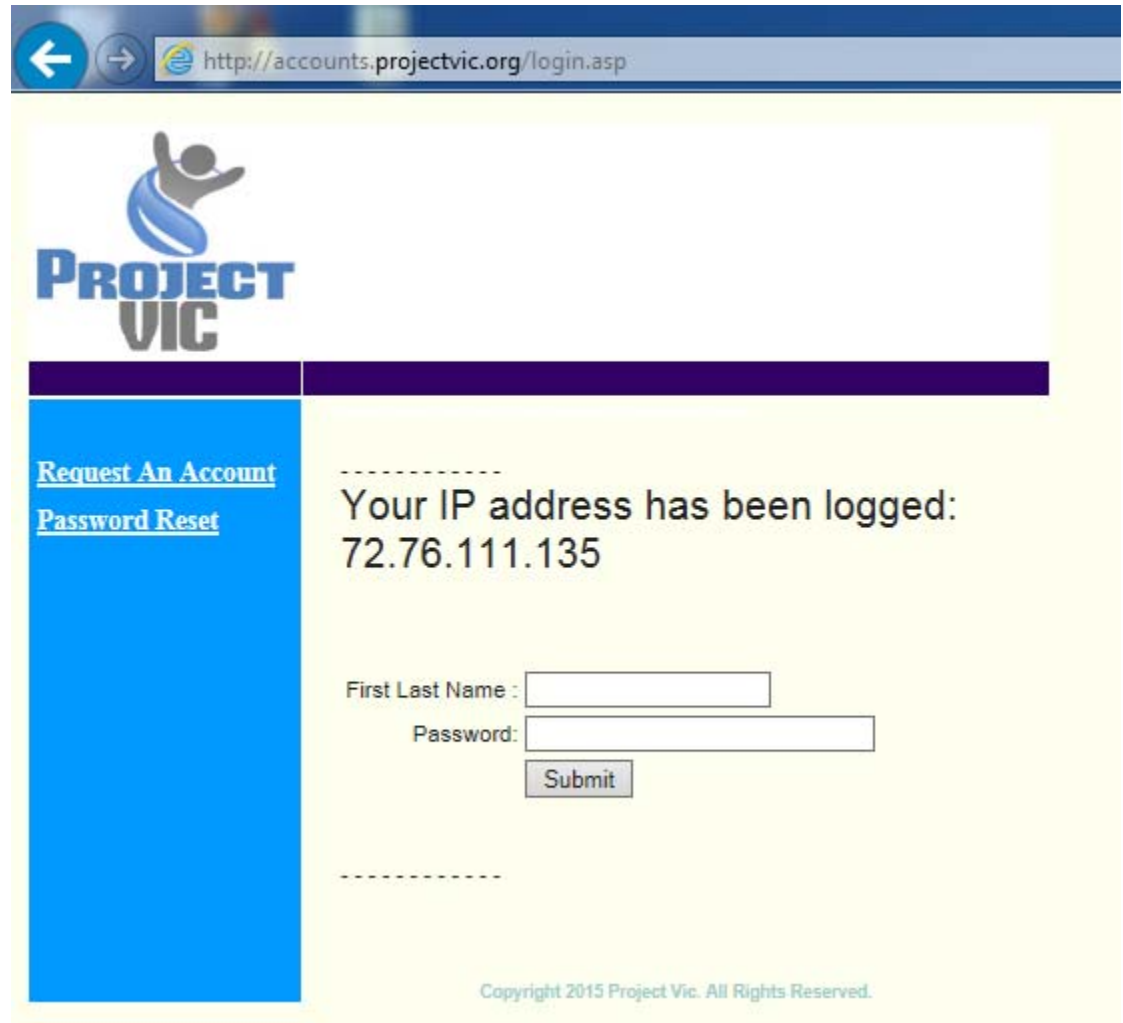
First Last Name :

Password:

Request Account

Copyright 2013 ICAC COPS. All Rights Reserved.

# Requesting a Project VIC Certificate

A screenshot of a web browser showing the Project VIC login page. The browser's address bar displays "http://accounts.projectvic.org/login.asp". The page features the Project VIC logo at the top left. Below the logo, there is a blue sidebar with two links: "Request An Account" and "Password Reset". The main content area is yellow and contains a message: "Your IP address has been logged: 72.76.111.135". Below this message are two input fields: "First Last Name :" and "Password:". A "Submit" button is located below the password field. At the bottom of the page, there is a copyright notice: "Copyright 2015 Project Vic. All Rights Reserved."

# Once Your Approved

---

## Project Vic Request Certificate

In order to access the Project Vic hashset, you must request a certificate. Upon making that request your ICACCops.com account manager will need to approve the request. Once approved, you will be able to download the certificate and install it. The password for the .pfx file will be your RoundUp Licence number.

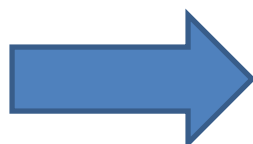
Certificate Requested on 8/11/2014 2:44:02 PM

Certificate Approved on 8/11/2014 2:44:51 PM

[Download Your Certificate](#)

[Instructions / Important Information](#)

[Hubstream / Netclean Webinars](#)



Certificate Password: 13a69f1e78afd500f2 [REDACTED] of

# Project Vic Hash Descriptions



## Proof of Concept Image Categorization Model 2012

Adopted Image Categorization Schema  
Dated-10/6/12

Background: The following is an image categorization "Schema" or Guide to be used by the participants of the "Proof of Concept Project" while the PoC is active. No agency is bound long term to this schema since this is a voluntary project.

- Hashes are to alert the investigator
- Images used to Prosecute should be reviewed by the prosecution.
- Local and Jurisdiction laws differ so reviews are crucial to the process.

Category #	Name	Description
0	Non-pertinent	All other files (These file hashes can be added to elimination sets)
1	Child Abuse Material (CAM)	Child Abuse Material (CAM) Material meeting the statutory definition of 18 USC 2256(8) – Content that depicts children engaged in sexually explicit conduct and/or the lewd and lascivious display of the genitalia. "Child Pornography" means any visual depiction, including photograph, film, video, picture depicting sexually explicit conduct. "Sexually explicit conduct" means material depicting any person under the age of 18 years engaged in graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast or pubic area of any person is exhibited. In addition any material depicting a minor involved in bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area.
2	Child Exploitive (non-CAM) / Age Difficult	Any material which when viewed on its own without reference to other material does not meet the definition of Category1 above. This category is used for material which indicates the exploitation of a child but does not meet the legal definition of child pornography. In addition age difficult and questionable material will be placed here.
3	CGI / Animation	Drawings, cartoons, animation, computer generated material (CGI), virtualization, stories, etc., which depict sexually explicit conduct with children.
4	Comparison Images	Search warrant photos and photos taken for comparison to Category 1 and 2 material.
5	Uncategorized	File category prior to categorization.

Tag and Series Management functions will be used to sub-categorize material for particular subsets of material and the tracking of series.

The tag "S&M/Violence" will be used to tag material that portrays sadistic or masochistic conduct or other depictions of violence.

The tag "Infant/Toddler" will be used to tag material which clearly depicts a pre-pubescent child who would be considered an infant or toddler.

# How Do I Sign Up for Project VIC

---



Lets take a look at the second entry point:

[www.icaccops.com/users](http://www.icaccops.com/users)

# Project Vic Participation

---

A screenshot of the Child Online Protective Services (COPS) website. The header includes a globe icon and the text "Child Online Protective Services" and "Making the Internet a Safer Place". A sidebar on the left contains links: "Home", "Req. Account", and "Please Read". The main content area has a large blue arrow pointing to a registration form with fields for "Name:", "Password:", and "Department (Do not abbreviate):".

*C hild  
O nline  
P rotective  
S ervices*

*Making the Internet a Safer Place*

○ Home  
○ Req. Account  
○ Please Read

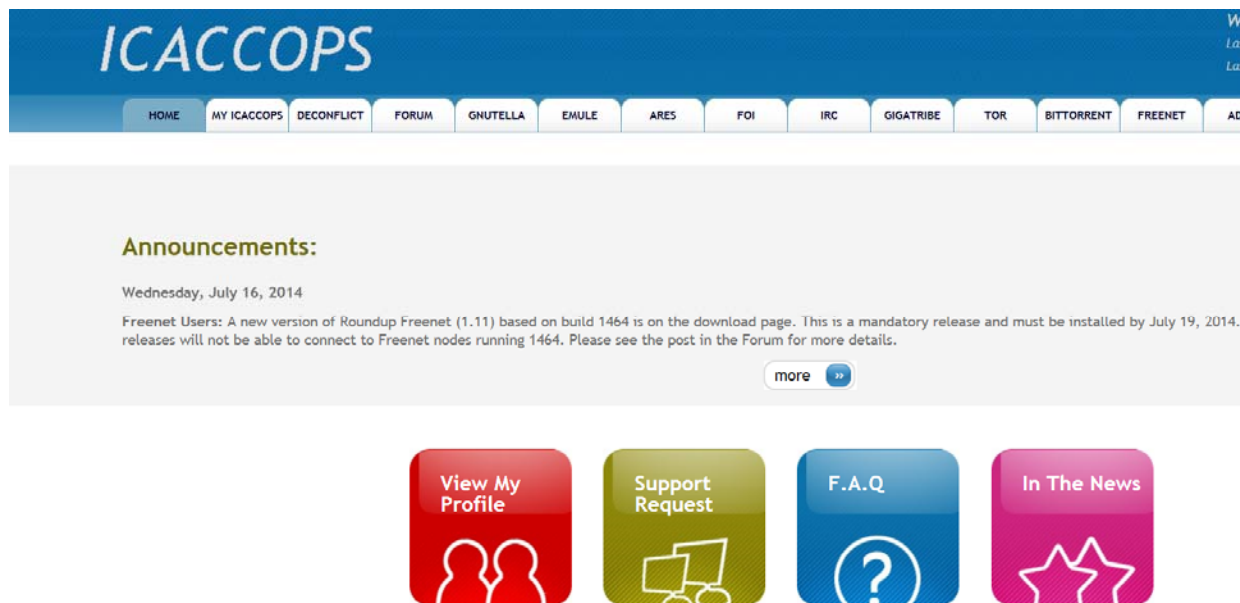
Name:  
Password:  
Department (Do not abbreviate):

- Fill out initial Registration Information and submit
- Wait for an email to notify you have been approved and follow the next steps

# Obtaining Access to Project Vic Hashes



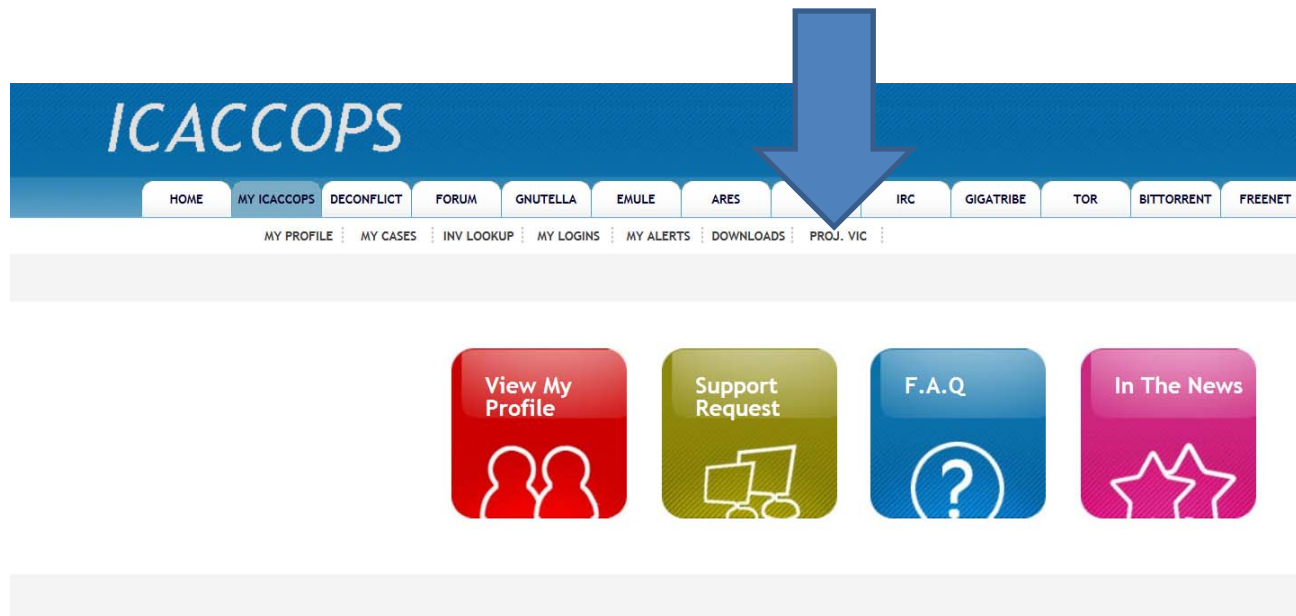
- Must have an account for the site



# Obtaining Access to Project Vic Hashes



- Look for Project Vic Tab



# Obtaining Access to Project Vic Hashes



- Request Certificate



# Obtaining Access to Project Vic Hashes

---



Thank you Richard Brown for requesting a Project Vic certificate.  
Upon submitting this form, your request will be sent to the appropriate account manager / ICAC Commander for approval.  
Upon it's approval, you will be informed via the email address associated with your ICACCops.com login.  
If no email is received, please contact your account manager / ICAC Commander.

Request Certificate



Request was submitted!  
Return to [Menu](#)

# Obtaining Access to Project Vic Hashes



- End user will now be able to download a user Certificate
- Instructions on Installation
- Guidance on the use of the hashes
- Categorization Schema.

The screenshot shows the ICACCOPS website interface. At the top is a blue header with the 'ICACCOPS' logo. Below the header is a navigation bar with tabs: HOME, MY ICACCOPS, DECONFLICT, FORUM, GNUTELLA, EMULE, ARES, and FOI. A secondary navigation bar contains links: MY PROFILE, MY CASES, INV LOOKUP, MY LOGINS, MY ALERTS, DOWNLOADS, and PROJ. VIC. The main content area is titled 'Project Vic Request Certificate' and contains the following text: 'In order to access the Project Vic hashset, you must request a certificate. Upon making that request your ICACCops.com account manager will need to approve the request. Once approved, you will be able to download the certificate and install it. The password for the .pfx file will be your RoundUp Licence number.' Below this text, it shows 'Certificate Requested on 8/11/2014 2:44:02 PM' and 'Certificate Approved on 8/11/2014 2:44:51 PM'. There are two blue links: 'Download Your Certificate' and 'Instructions / Important Information'.

# Obtaining Access to Project Vic Hashes



There is a waiting period of 24-48 hours before the created personal Certificate gets approved by the cloud administrator.

Once approved you can follow the next steps



## [Main Menu](#)

User Name  
Organization  
Telephone Number  
Email Address  
Password

Richard Brown  
NJSP Retired Now ICMEC  
5712305576  
rbrown@icmec.org  
13a69f1e78afd500f2753bcee08e230f

Create User



# Obtaining Access to Project Vic Hashes

---



- Upon Authorization by an ICACCOPS Administrator you will be able to download your Encryption Certificate from your ICAC COPS Account.
- You will not be able to install the certificates until they are populated into the cloud service by the Cloud Administrator ( 24-48 hours)
- Password for your personal certificate will be your ICAC Account Roundup License # under "My Profile"
- Install the service agent and it will download the hashes.

# Installing the Cloud Client



[www.hubstreamonline.net](http://www.hubstreamonline.net)



HOME

## Install Agent

Hubstream Intelligence Agent synchronizes data between Hubstream Intelligence and other systems. Agent requires valid credentials and a connection to one or both of Intelligence Fabric cloud service or Intelligence Server on-premises server. The following prerequisites are required:

- Windows Installer 4.5
- Microsoft .NET Framework 4

[INSTALL NOW](#)

## Service Updates

July 17, 2015 (version 2.5.356)

Support for version 1.2

Files exported from new versions of tools that support the 1.2 data model can be uploaded

February 22, 2015 (version 2.5.208)

Support for version 1.2

Files can be downloaded in 1.2 format by changing the data model setting to 1.2 (note that Default is still set to 1.1 to support older tools)

Performance improvements

Faster startup times

Improved upload handling for slow networks

January 11, 2015

Support SSL so that the Hubstream certificate install is no longer required

August 25th, 2014

Improved download

# Installing the Cloud Client



## Install Agent

Hubstream Intelligence Agent synchronizes data between Hubstream Intelligence and other systems. Agent requires valid credentials and a connection to one or both of the Fabric cloud service or Intelligence Server on-premises server. The following prerequisites are required:

- Windows Installer 4.5
- Microsoft .NET Framework 4

 **INSTALL NOW**

## Service Update

July 17, 2015 (version 2)

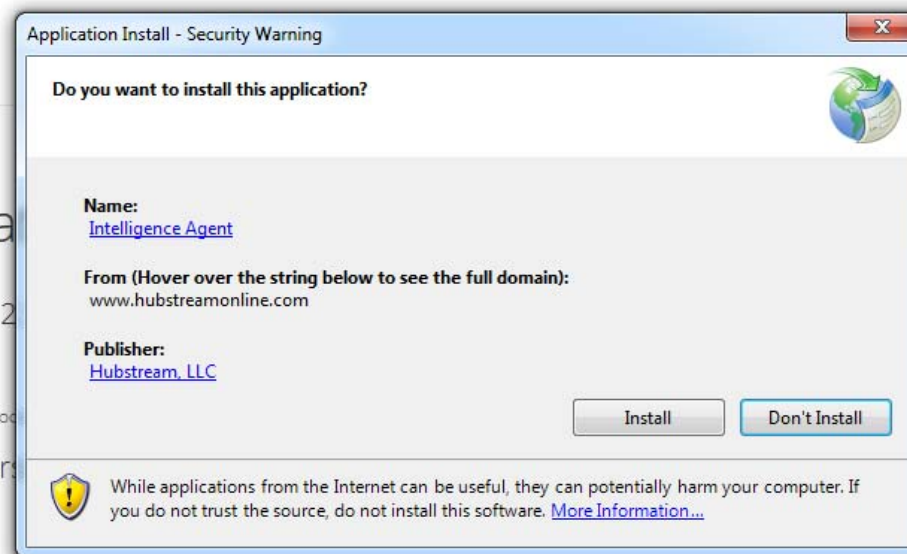
Support for version 1.2

Files exported from new versions of tool

February 22, 2015 (version 1.1)

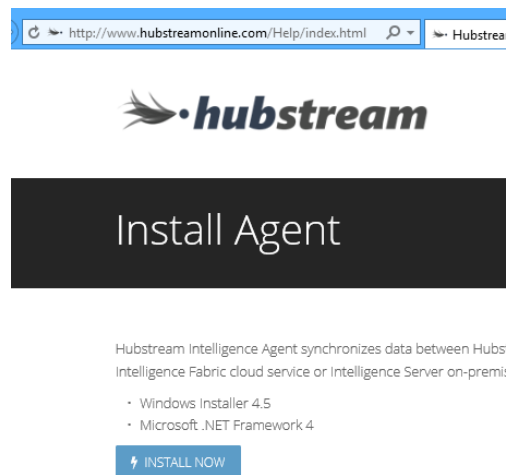
Support for version 1.2

Files can be downloaded in 1.2 format by changing the data model setting to 1.2 (note that Default is still set to 1.1 to support older tools)





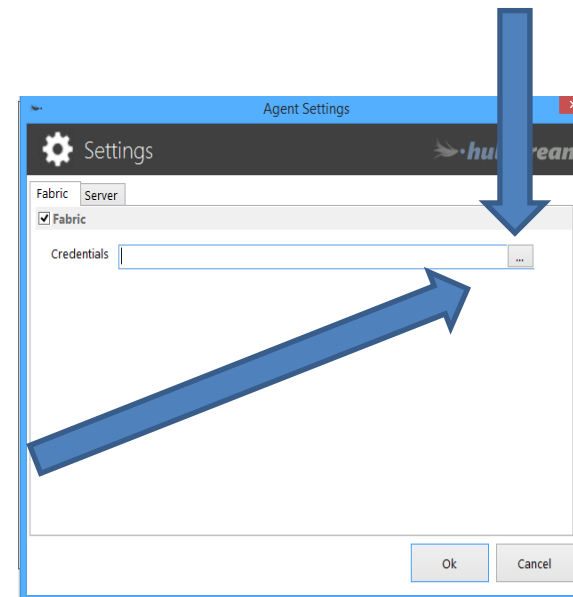
Now you are ready to install the agent and your personal certificate



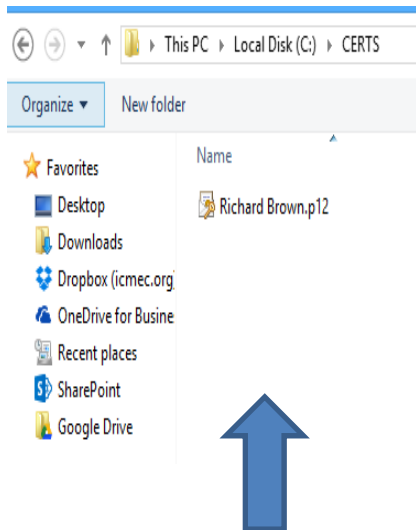
Go to [www.hubstreamonline.com/help/index.html](http://www.hubstreamonline.com/help/index.html) and install the service agent.

Once installed open the service agent in order to load your personal credential

Hit the Browse button



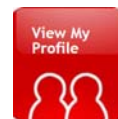
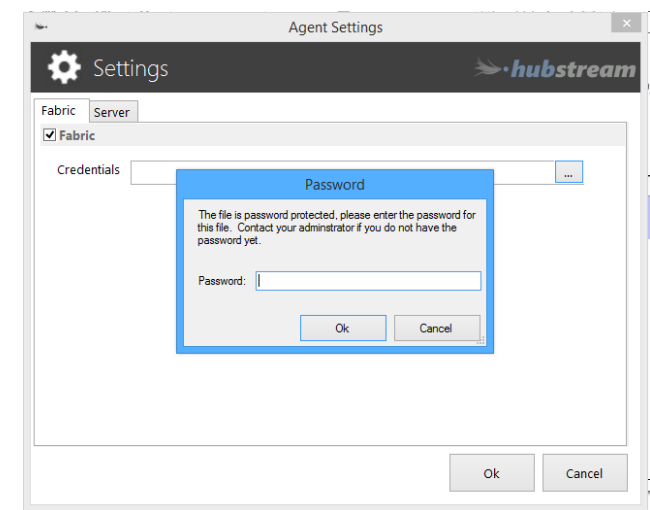
# Signing up for Project Vic Hashes



Once you browse to your downloaded personal certificate.

Double click and you will be asked for your password

Remember your password is your ICACCOPS Roundup License listed in your profile



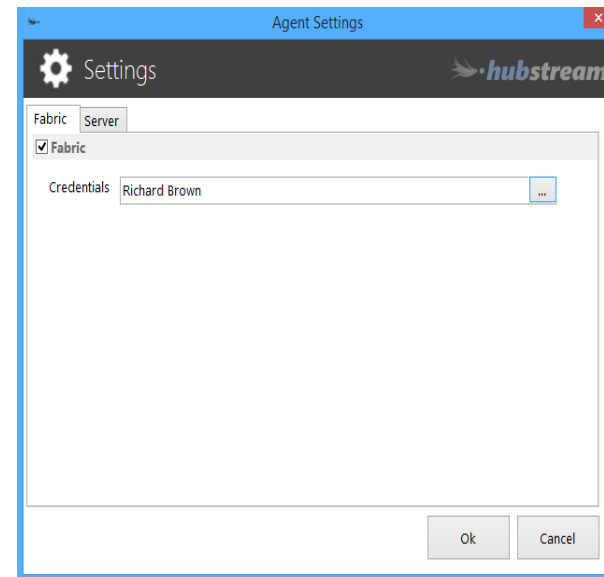
Roundup License:	13a69f1e78afd500f2753bcee
Name:	Richard Brown
Department:	NJSP Retired Now ICMEC
Street:	1700 Diagonal Rd
City:	Alexandria
State:	VA
Zip:	22314
Phone:	7323951640
Email:	rbrown@icmec.org
Taskforce Area:	ICMEC
<button>Update record</button>	

# Signing up for Project Vic Hashes

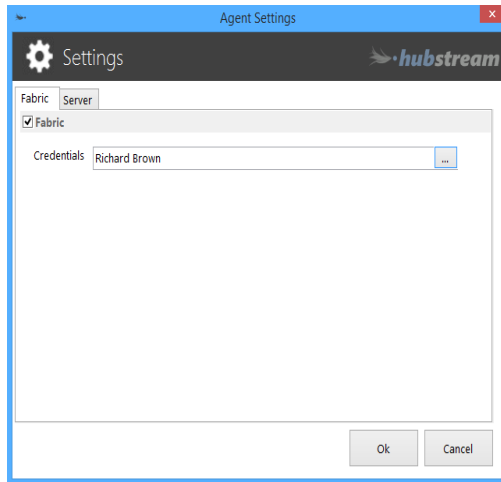


If you see the red asterisk

- Your Certificate may not be registered with the cloud service yet

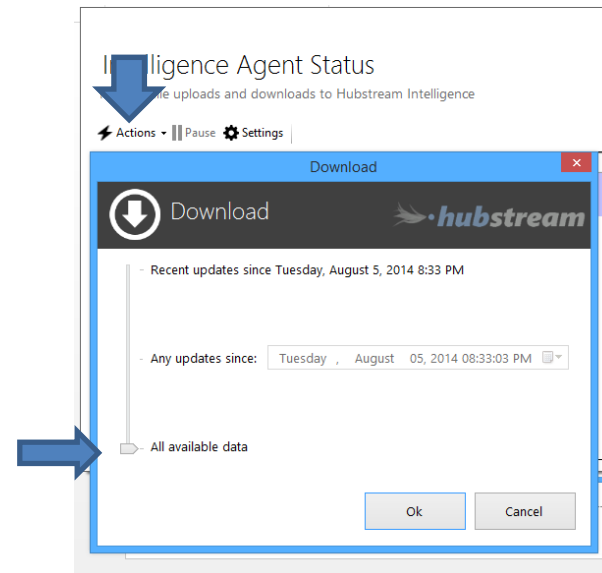


# Signing up for Project Vic Hashes



Once the agent has taken your credentials you are ready for the initial download.

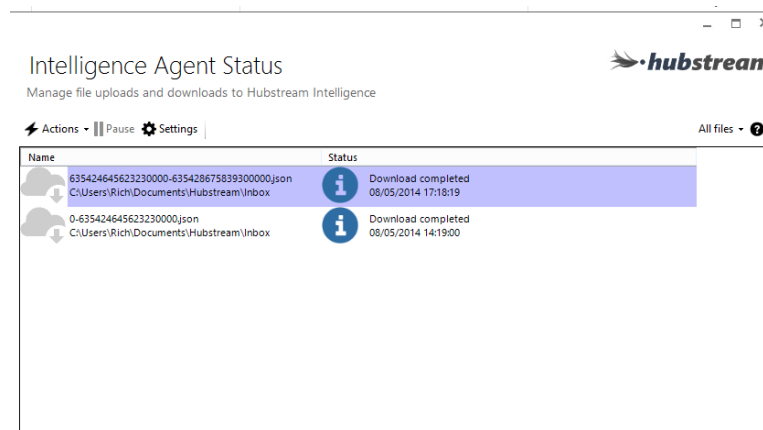
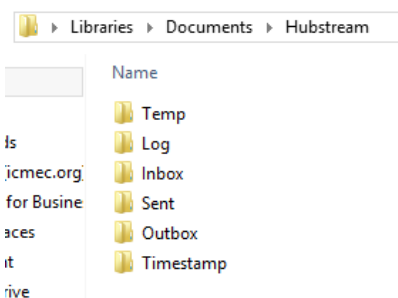
Go to the "Actions" tab and have the agent "download all available Data"



# Accessing Your Project VIC Hashes



- Hashes will stream down and decrypt with your certificate .
- The service will use a series of folders to organize the hashes .



# The VICS Hash Record

```

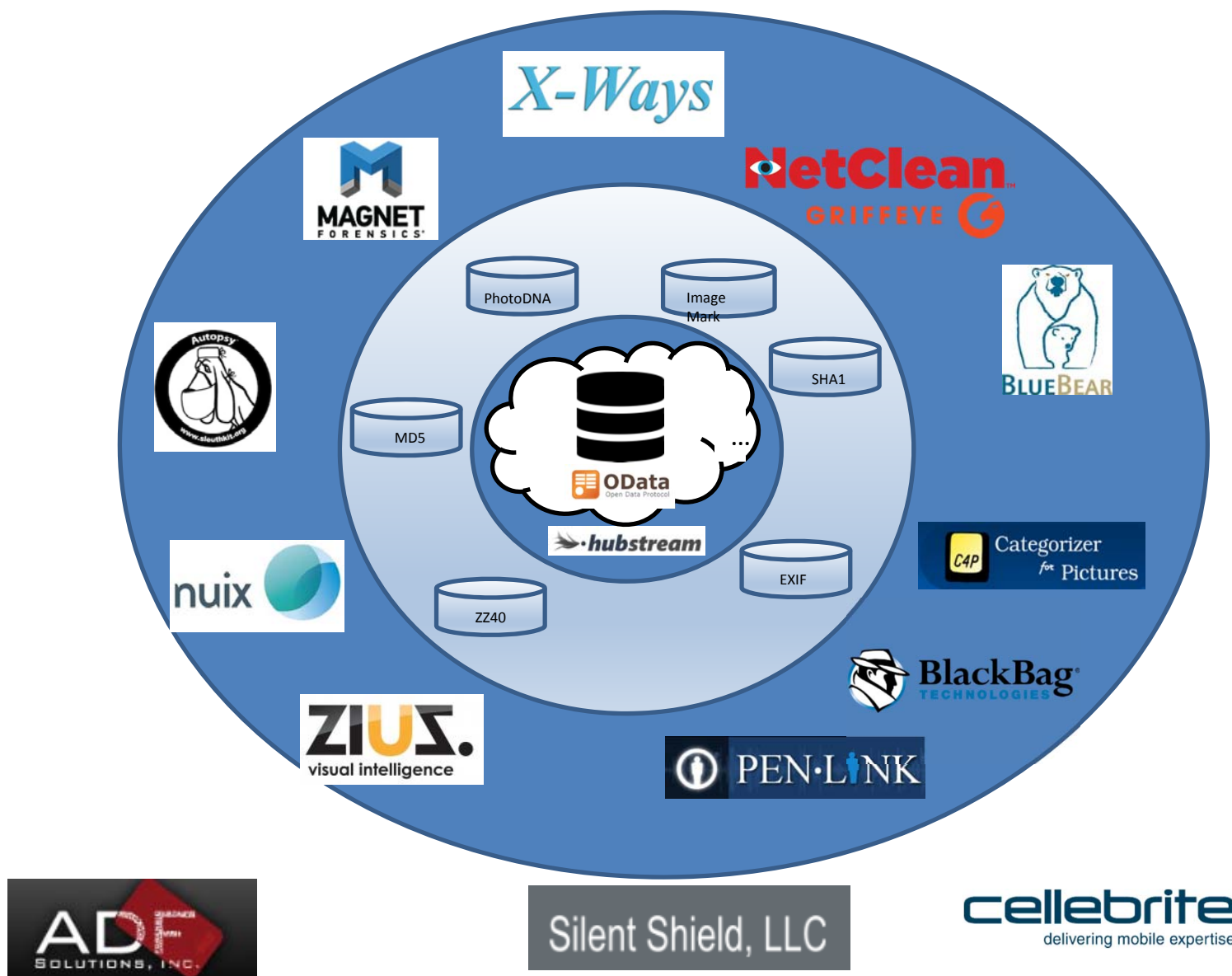
"odata.id":"Media(\"30228\")", "odata.editLink":"/Media(30228)", "AlternativeHashes@odata.navigationLinkUrl":"/Media
(30228)/AlternativeHashes", "AlternativeHashes":[
  {
    "odata.editLink":"/AlternativeHashes
    (HashName='PhotoDNA',MediaID=30228)", "Media@odata.navigationLinkUrl":"/AlternativeHashes
    (HashName='PhotoDNA',MediaID=30228)/Media", "MediaID":30228, "HashName":"PhotoDNA", "HashValue":"QjijbPya20K3IILnZ0Wpn0qJgPAgqd47Vb
    Y1QnCjobMd43bWBRBV8boY+RAZB1Xc20xMkTiXZm+mldXQINR0ZSEg4wv1XCzJV5vgNEXAzVpm3aT90Co67EFEKSGPynFhuVHRHNR/E7m1019DvF
    +MCx5jd0IXfUCPp3kVZm51V9ff0/kHXIYJD94bCBJKpvST7j5sokvwjpaD2oop0YxjtbjoUJgP517iA7Cb16TAfmk63TuuK0k5mTg74zFxfh"
  }
], "Exifs@odata.navigationLinkUrl":"/Media(30228)/Exifs", "Exifs":[
  {
    "odata.editLink":"/Exifs(MediaID=30228,PropertyName='Make')", "Media@odata.navigationLinkUrl":"/Exifs
    (MediaID=30228,PropertyName='Make')/Media", "MediaID":30228, "PropertyName":"Make", "PropertyValue":"NIKON"
  },{
    "odata.editLink":"/Exifs(MediaID=30228,PropertyName='Model')", "Media@odata.navigationLinkUrl":"/Exifs
    (MediaID=30228,PropertyName='Model')/Media", "MediaID":30228, "PropertyName":"Model", "PropertyValue":"COOLPIX P300"
  },{
    "odata.editLink":"/Exifs(MediaID=30228,PropertyName='Software')", "Media@odata.navigationLinkUrl":"/Exifs
    (MediaID=30228,PropertyName='Software')/Media", "MediaID":30228, "PropertyName":"Software", "PropertyValue":"COOLPIX P300 V1.0"
  },{
    "odata.editLink":"/Exifs(MediaID=30228,PropertyName='CreateDate')", "Media@odata.navigationLinkUrl":"/Exifs
    (MediaID=30228,PropertyName='CreateDate')/Media", "MediaID":30228, "PropertyName":"CreateDate", "PropertyValue":"2013:06:07
    03:52:09"
  }
], "MediaID":30228, "Name":"DSCN0649.JPG", "Category":3, "Comments":"","Identified":false, "IsDistributed":false, "MD5":"6E7517568E6341
02FE3D12074608E76A", "Series":"","SHA1":"44DC371B7E8EA0FD6BF6985ED5DB9CCA26D70160", "Tags":""
},{
  "odata.id":"Media(\"30229\")", "odata.editLink":"/Media(30229)", "AlternativeHashes@odata.navigationLinkUrl":"/Media
  (30229)/AlternativeHashes", "AlternativeHashes":[

```

# Our Tools

---

- Media Tools allow us to closely examine Images and Video and leverage the attached Meta-Data.
- These tools complement your forensic tools and allow for a closer examination of the media, allowing for categorization work and Victim ID practices.



## Beyond the Grid, AnalyzeDI 15.1

Now with Analyze Relations



## NetClean Forensic Market

Download apps and buy support to enhance the functionality of NetClean Analyze to get the maximum out of your installation.

### Hex Viewer

View files in the embedded Hex Viewer



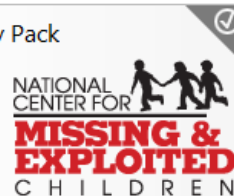
### VICS (OData)

Import and Export



### NCMEC Utility Pack

Prepares files for submission to NCMEC's Child Victim Identification program (CVIP)



### Reverse Geocoding

Converts GPS coordinates to a physical address





# BlueBear LES



Confirm Evidence Media Files

Record Set: 1

Filter: Category | Exif | Filename | File Attribute | Comment | User | Option | File Property | Sort Option | Match

Case ID: 9 : "Test3"

Evidence ID (Optional):

File ID (Optional): 0

Find Similar Images Within Case

Filter

Retrieve Data

Statistics

Category	Gall...	All
1- Child Abuse	2	2
2- Child Exploiti...	2	2
3- CGI / Anima...	0	0
4- Comparison ...	0	0
6- Non-Pertinent	0	0
AICS	0	0
Unknown	4	4

Gallery | Image | Related Evidence Media Files | Image Details | Directory | Directory Statistics

1 2 1 0 0 0 0 0

Filename Real Path: 1 - C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg

1 / 8 (Page 1 / 1)

ff ( #0357 )

Import Export Search Optio

- Basic Hash File
- Hash Keeper
- Lace Database
- Interpol Hash
- CETS Hash
- Swiss National Hash
- Project Vic OData Hash

57 )

Export Search Options Lang

- Type 1 Export Hash Set
- CETS Export
- PhotoDNA Export
- Project Vic OData Hash

# Magnet IEF

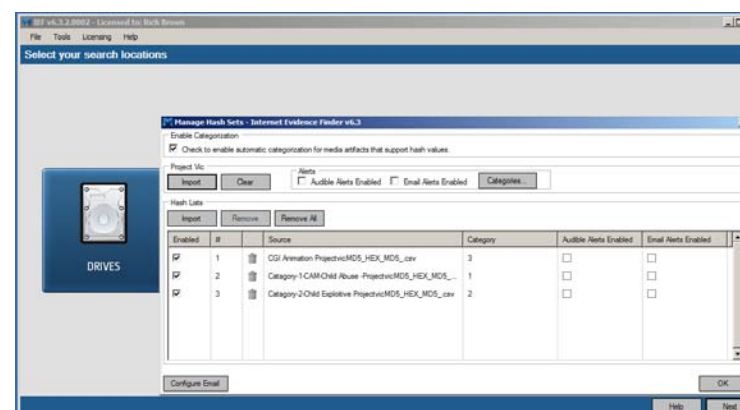


Project Vic

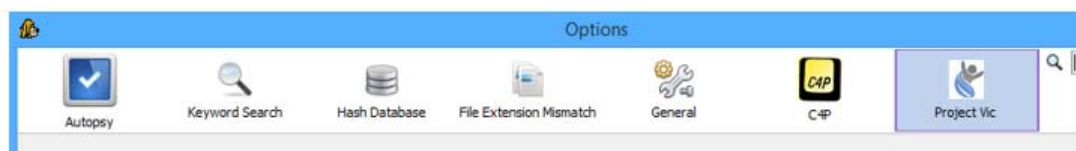
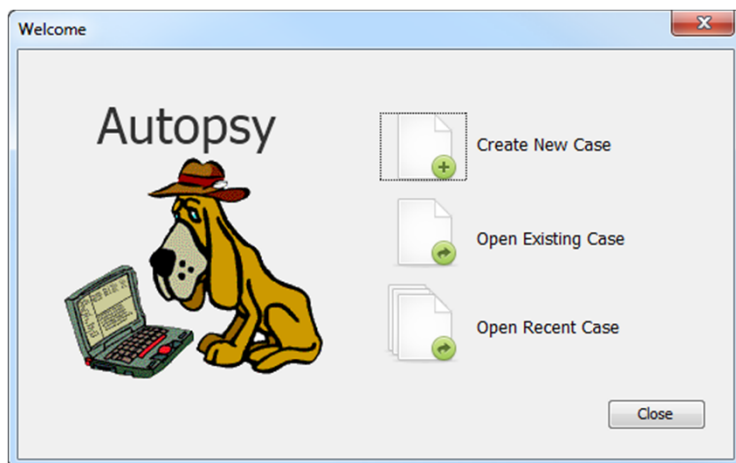
Import Clear

Alerts

☐ Audible Alerts Enabled ☐ Email Alerts Enabled Categories...



# Autopsy



Category	Filename
Project Vic Cat 0: Uncategorized	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_0.kdb
Project Vic Cat 1: Child Exploitation Material (Illegal)	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_1.kdb
Project Vic Cat 2: Child Exploitation Material (Non-Illegal/Age ...	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_2.kdb
Project Vic Cat 3: CGI/Animation Material (Child Exploitive)	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_3.kdb
Project Vic Cat 4: Exemplar/Comparison Material (Internal Use...	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_4.kdb
Project Vic Cat 5: Non Pertinent Material	C:\Users\Rich\Documents\Autopsy Hash\ProjectVic_5.kdb

## Module for Autopsy

### Law Enforcement Bundle

Integration with Project Vic and C4P/All databases for sharing image and video categorizations

# BlackBag



**BlackBag**<sup>®</sup>  
TECHNOLOGIES

Saved Filters:

Select where **all** of the conditions are met:


Kind: **Graphics - All**

Date Created: **is after** **1/ 1/10**

Hash Set: **Files Not In Has...** **Known OS X System Files**

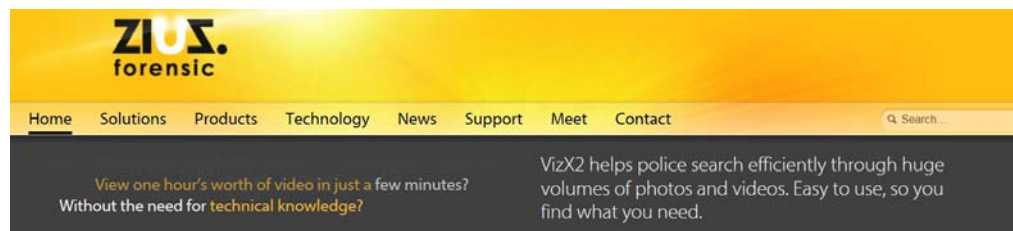
Size: **is greater than** **500** **KB**

ID	Name	Size	Date Created	Date Modified	Date Accessed	Extension	Content E...	Path
5054...	96f9ca7a539f4c5759a1df67...	1.3 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5054...	500534f621536ba4a097137...	1.2 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5054...	2a541bf473c7a136df7b42...	1.1 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5055...	c020c53266390e07490c0f...	1.2 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5055...	35c3379ecf98423a140978f5...	1.3 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5055...	6c6a11061d58465ae68429b...	1.2 MB	2010-11-30 (UTC)	2010-11-30 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
1728...	2010-12-01 12.20.03.jpg	1.3 MB	2010-12-01 (UTC)	2010-12-01 (UTC)	2013-05-06 (UTC)	JPG		/Users/josh/Dropbox/Camera Uploads/20
1728...	2010-12-01 12.20.07.jpg	1.3 MB	2010-12-01 (UTC)	2010-12-01 (UTC)	2013-05-06 (UTC)	JPG		/Users/josh/Dropbox/Camera Uploads/20
1728...	2010-12-01 12.21.18.jpg	1.2 MB	2010-12-01 (UTC)	2010-12-01 (UTC)	2013-05-06 (UTC)	JPG		/Users/josh/Dropbox/Camera Uploads/20
1728...	2010-12-01 12.21.23.jpg	1.1 MB	2010-12-01 (UTC)	2010-12-01 (UTC)	2013-05-06 (UTC)	JPG		/Users/josh/Dropbox/Camera Uploads/20
5095...	55eee8d00fea75cbeaae8d9...	1.3 MB	2010-12-02 (UTC)	2010-12-02 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f
5096...	e9aa7302d325eeadd7080...	1.2 MB	2010-12-02 (UTC)	2010-12-02 (UTC)	2012-04-09 (UTC)	JPG		/Users/josh/Library/Application Support/f



(1 of 113) - /acer/Users/josh/Dropbox/Camera Uploads/2010-12-01 12.20.03.jpg

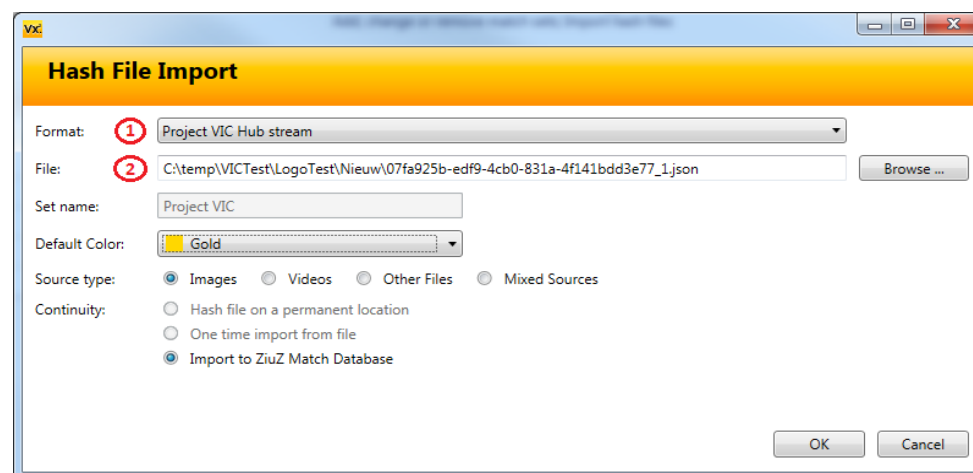
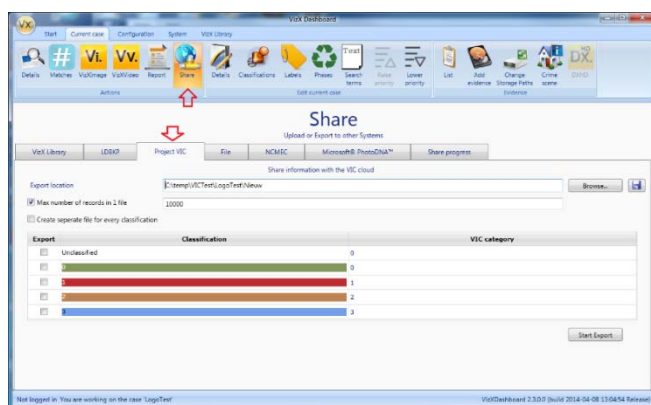
# ZIUZ Supports Project VIC OData/Json Hash Sets

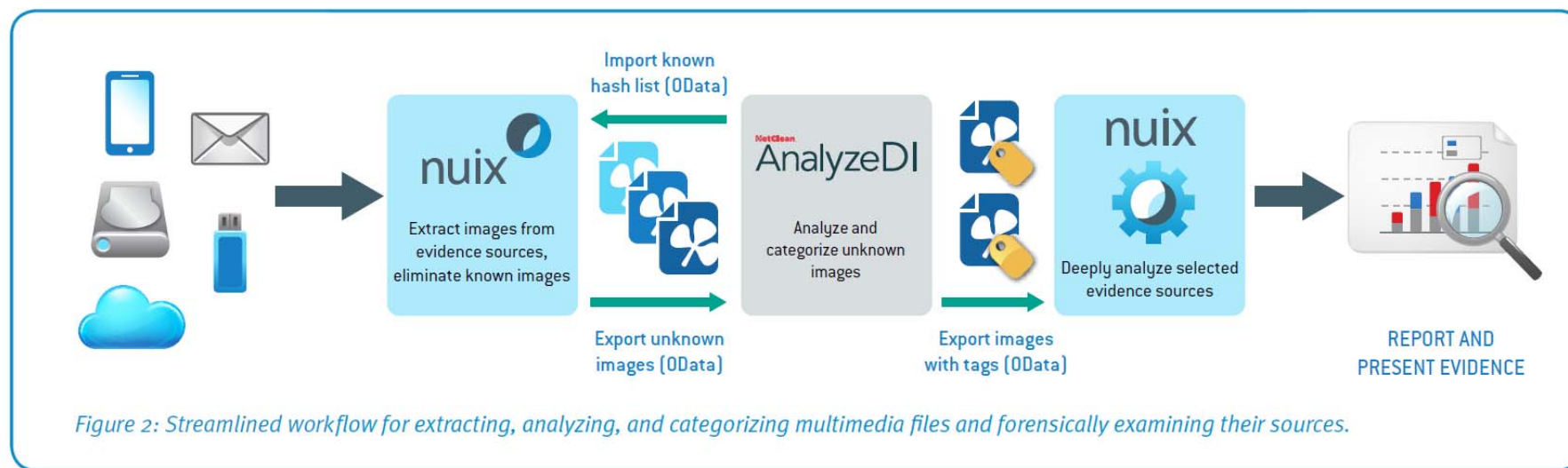


**VizX2**

Ziuz VizX 2 is a total solution for analysing large amounts of video and photo material confiscated in police investigations.

**Try it yourself**  
Request a 90-day trial





---

# *X-Ways*

- X-Ways Version 18.2 or higher supports Project VIC and the “VICS” Data Model



- Import Project VIC Hashes into Pen-Link 8



# Post Webinar Information

---

- At the conclusion of the webinar, a short survey will appear. We ask that you complete the survey in an effort to gather information to better serve the community in preparation for future webinars. Please complete it before signing off.
- You will receive a link to access our law enforcement only webinar library where you can view the recording and access related webinar material. Due to the sensitivity of some of the material you must be a registered law enforcement member of the *NCJTC.org* or *ICACTaskforce.org* websites. If you are not currently a member, you will need to register for access at [www.ncjtc.org](http://www.ncjtc.org).

# Additional Information

---

*Points of view or opinions expressed in this webinar are those of the presenter(s) and do not necessarily represent the official position or policies of OJJDP or the U.S. Department of Justice.*