



# Easily Create SCAP Content with the MACE Wizard Tool

Tina Ackerman  
DoD  
September 27, 2010



# Definitions



- **SCAP (S-CAP)** – “Security Content Automation Protocol” is a standard way of documenting server configurations and descriptions of malware in a machine readable form. A suite of XML document specifications and other standards used to develop a common way to assess compliance and vulnerability issues.
- **XML**- eXtensible Markup Language
- **OVAL** – Open Vulnerability and Assessment Language: Standard XML based language for expressing the necessary logic to check for vulnerabilities, compliance, installed software and patches.



# Definitions cont.



- **XCCDF-** Extensible Configuration Checklist Description Format. It is XML for specifying checklists and for reporting results of checklist evaluation. An XCCDF benchmark defines a number of rules who generally reference definitions in an OVAL.xml document.
- **CPE- Dictionary.xml-** A dictionary consisting of two files, a CPE-Dictionary.xml and CPE OVAL.xml. CPE-Dictionary.xml contains targeted platforms and references the file containing the platform inventory definitions/checks.
- **CPE- OVAL.xml-** Is an accompanying file of the CPE Dictionary.xml file. It includes the platform OVAL check(s) for determining applicability of the benchmark definitions.



# Malware Content Editor (MACE) 1.0



- **Wizard Mode-** designed for automated SCAP content generation of XCCDF wrapped OVAL SCAP content without requiring users to fully understand XML, XCCDF, or OVAL. This mode provides a limited set of features.
- **Standard Mode-** considered an advanced feature, for example, editing OVAL and XCCDF documents/files.



# Malware Content Editor (MACE) 1.0



- **Purpose:**

To provide step-by-step instruction on how to create an SCAP data stream (OVAL, XCCDF, CPE – Dictionary.xml, and CPE- OVAL.xml) to search for and discover artifacts on an operating system.



# Malware Content Editor (MACE) 1.0



- **Per National Institute of Standards and Technology (NIST) 800-126**
- **SCAP Data Stream**
  1. OVAL.xml
  2. XCCDF.xml
  3. CPE- Dictionary.xml
  4. CPE- OVAL.xml



# Content Creation



- **PART 1** - Create SCAP Data Stream for a Single OVAL file.
- **PART 2** - Create SCAP Data Stream for Multiple OVAL files.



## PART 1

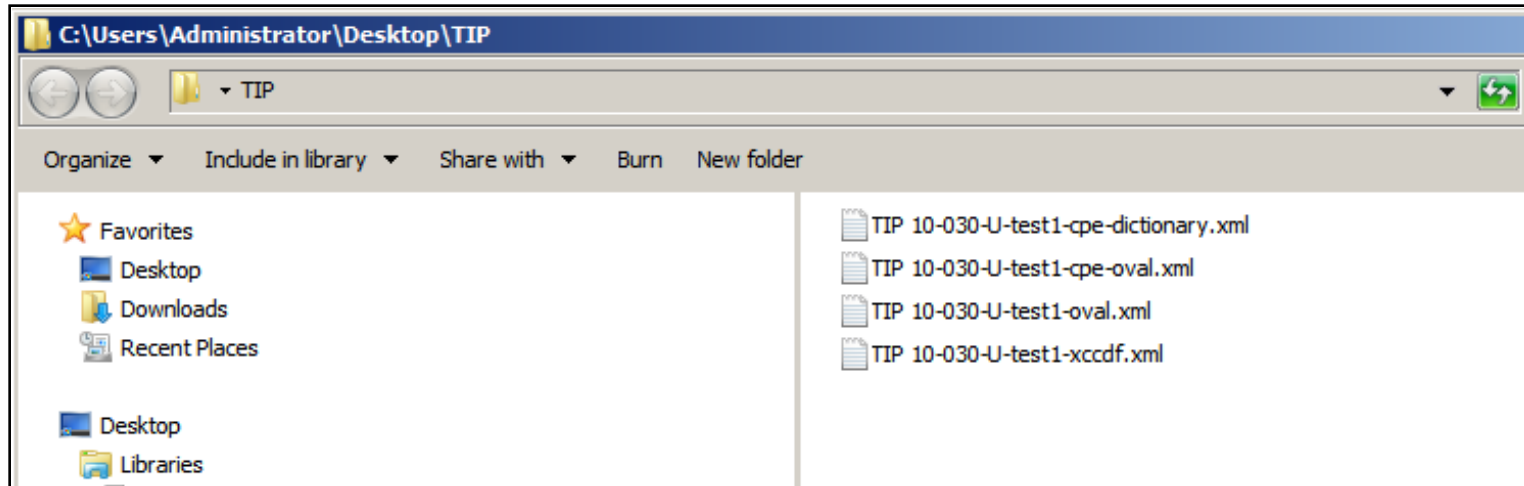


# OVAL Creation for a File





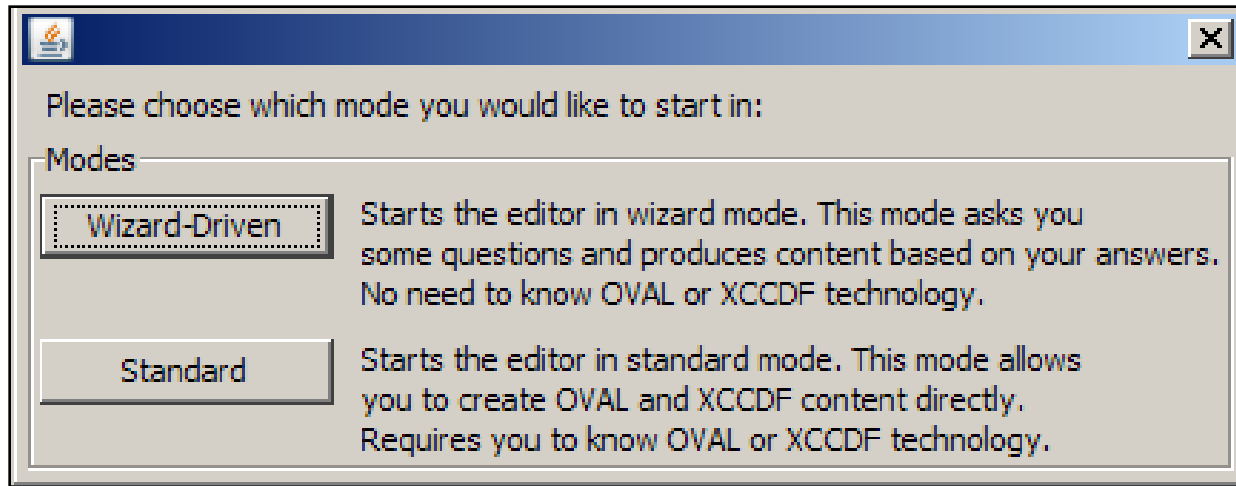
# OVAL Creation (for a file)



**Create SCAP Data Stream for a Single OVAL check**



# OVAL Creation (for a file)





# OVAL Creation (for a file)



**Malware Content Editor(Wizard Mode)** [X]

Target OVAL version

1 OVAL\_53 [v]

OVAL Namespace Identifier

2 DOD.DIB.gov

What would you like to create?

3 File(windows) - Creates file/directory related content. [Go!]  
File(unix) - Creates file/directory related content.  
Registry - Creates windows registry related content.



# OVAL Creation (for a file)



**Create New windows File Test**

What to check about file

Platform windows

Title

Path

Regex

%appdata%  
%commonprogramfiles%  
%commonprogramfiles(x86)%  
%homedrive%  
%homepath%  
%programdata%  
%programfiles%  
%programfiles(x86)%

File detail

Must exist and meet the following criteria

path(String)  
filename(String)  
owner(String)  
size(Int)  
a\_time(Int)  
c\_time(Int)  
m\_time(Int)  
ms\_checksum(String)  
version(/EP/STOM)

Added

Page 1 of 2



# OVAL Creation (for a file)



Create New windows File Test

What to check about file

Platform windows

Title  
TIP 10-030-U favorites.dat, variable path, MD5

Path  
C:\  Regex

Filename  
favorites.dat  Regex

Recurse to find file(s)/directory(ies)

Direction down Depth Unlimited

File/Dir Existence  
 Exists  Doesn't Exist

File detail  
 Must exist and meet the following criteria

path(String)  
filename(String)  
owner(String)  
size(Int)  
a\_time(Int)  
c\_time(Int)  
m\_time(Int)  
ms\_checksum(String)  
version/ERSTOM

Added

Page 1 of 2



# OVAL Creation (for a file)



Create New windows File Test

What to check about file

Platform windows

Title  
TIP 10-030-U favorites.dat, variable path, MD5

Path  
C:\  Regex

Filename  
favorites.dat  Regex

Recurse to find file(s)/directory(ies)  
Direction  Depth

File/Dir Existence  
 Exists  Doesn't Exist

File detail  
 Must exist and meet the following criteria  
development\_class(String)  
company(String)  
internal\_name(String)  
language(String)  
original\_filename(String)  
product\_name(String)  
product\_version(String)  
md5(String)  
sha1(String)

Added

Page 1 of 2



# OVAL Creation (for a file)



The screenshot shows a 'Create New windows File Test' dialog box with a 'Save' dialog box overlaid. The 'Create New windows File Test' dialog box has a 'What to check about file' tab selected, showing an 'Overview' section with instructions: 'Please choose a filename for your new OVAL content. If you choose an existing file it will be overwritten. An accompanying XCCDF document will also be created that references the checks you created in the OVAL content.' Below this is a text field for the filename with the instruction 'Filename must end in '-oval.xml'' and a 'Browse' button. The 'Save' dialog box is open, showing the 'Save in:' dropdown set to 'TIP 10-030'. The 'File name:' field contains 'TIP 10-030-U-test1'. The 'Files of type:' dropdown is set to 'All Files'. The 'Save' button is highlighted. At the bottom of the 'Create New windows File Test' dialog box, there are 'Back', 'Finish', and 'Cancel' buttons. The page number 'Page 2 of 2' is visible in the bottom left corner.



# OVAL Creation (for a file)



**Create New windows File Test**

What to check about file | Save content

Overview

Please choose a filename for your new OVAL content. If you choose an existing file it will be overwritten. An accompanying XCCDF document will also be created that references the checks you created in the OVAL content.

Filename must end in '-oval.xml'

C:\Users\Administrator\Desktop\TIP 10-030\TIP 10-030-U-test1-oval.xml

Status The file name is valid.

Page 2 of 2

Xccdf automatically generated





# OVAL Creation (for a file)



**Malware Content Editor(Wizard Mode)**

Target OVAL version  
OVAL\_53

OVAL Namespace Identifier  
DOD.DIB.gov

What would you like to create?

File(windows) - Creates file/directory related content.  
File(unix) - Creates file/directory related content.  
Registry - Creates windows registry related content.

Go!



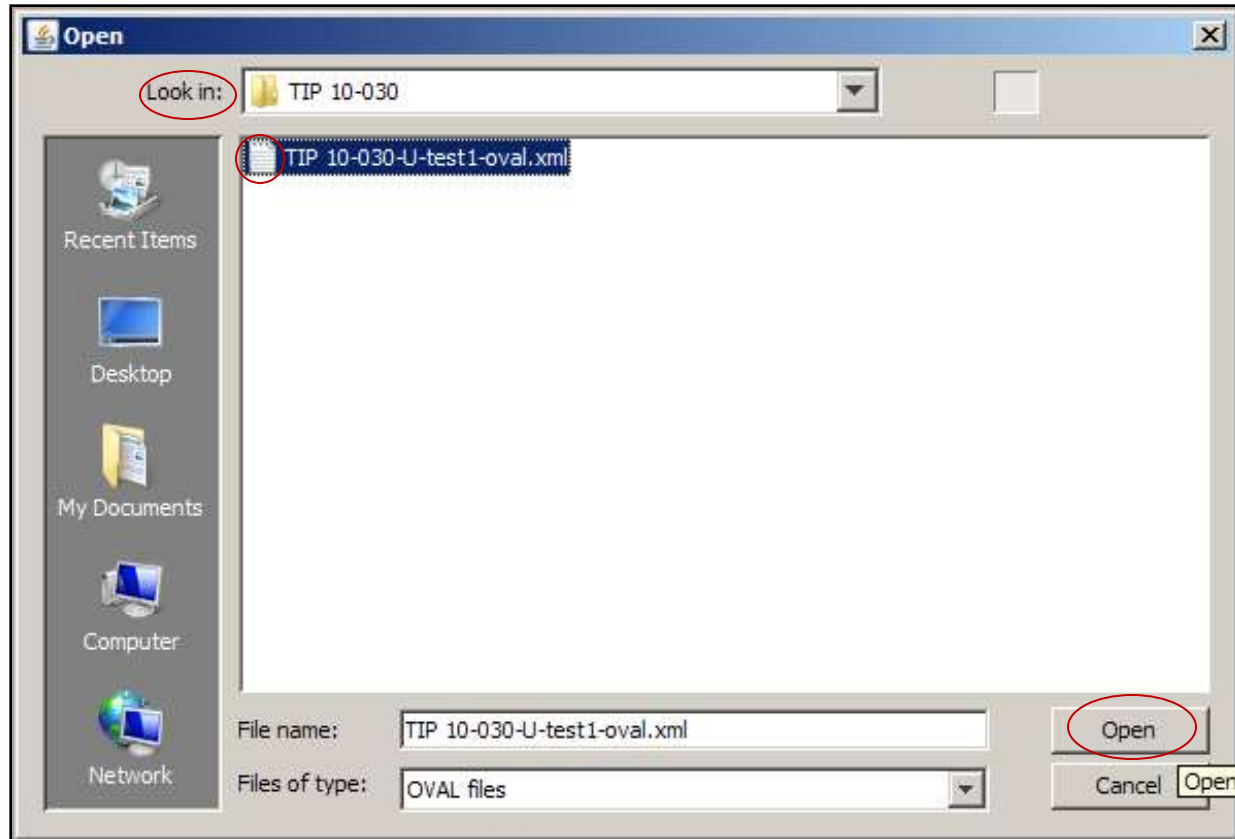
## PART 1



# OVAL Content Verification



# OVAL Content Verification



**In Standard Mode**



# OVAL Content Verification



The screenshot displays the Malware Content Editor 1.0 interface. The main window shows an OVAL Document with a tree view on the left and a detailed view on the right. The tree view includes folders for Definitions, Tests, Objects, and States, with specific OVAL objects selected. The right pane shows the configuration for an OVAL Object (oval:DOD.DIB.gov:obj:1), including its ID, type (filehash\_object), version (1), and comment. The 'Use Behaviors' section is checked, and the 'Behaviors' list includes 'recurse\_direction = down' and 'max\_depth = -1'. The 'Structure for OVAL Object' section shows parameters for path and filename. A red circle highlights the 'Expand All' button in the bottom left corner of the tree view.

1



# OVAL Content Verification



The screenshot displays the Malware Content Editor 1.0 interface. The main window shows an OVAL Document with a tree view on the left and a configuration panel on the right. The configuration panel is set to the 'State' tab and shows the following details:

- State Id: oval:DOD.DIB.gov:ste:1
- State Type: filehash\_state
- Version: 1
- Comment: Check files for md5 equals C5AD3523C84261D718Aff32AE7453fde
- Possible parameters: path
- Added parameters table:

Name	Operation	Datatype	Value	
md5	equals	string	C5AD3523C84261D718Aff32AE7453FDE	Edit Remove

The 'Value' column header in the table is circled in red. The interface also includes a search bar, a style dropdown, and a messages pane at the bottom.

**File > Save for any changes**



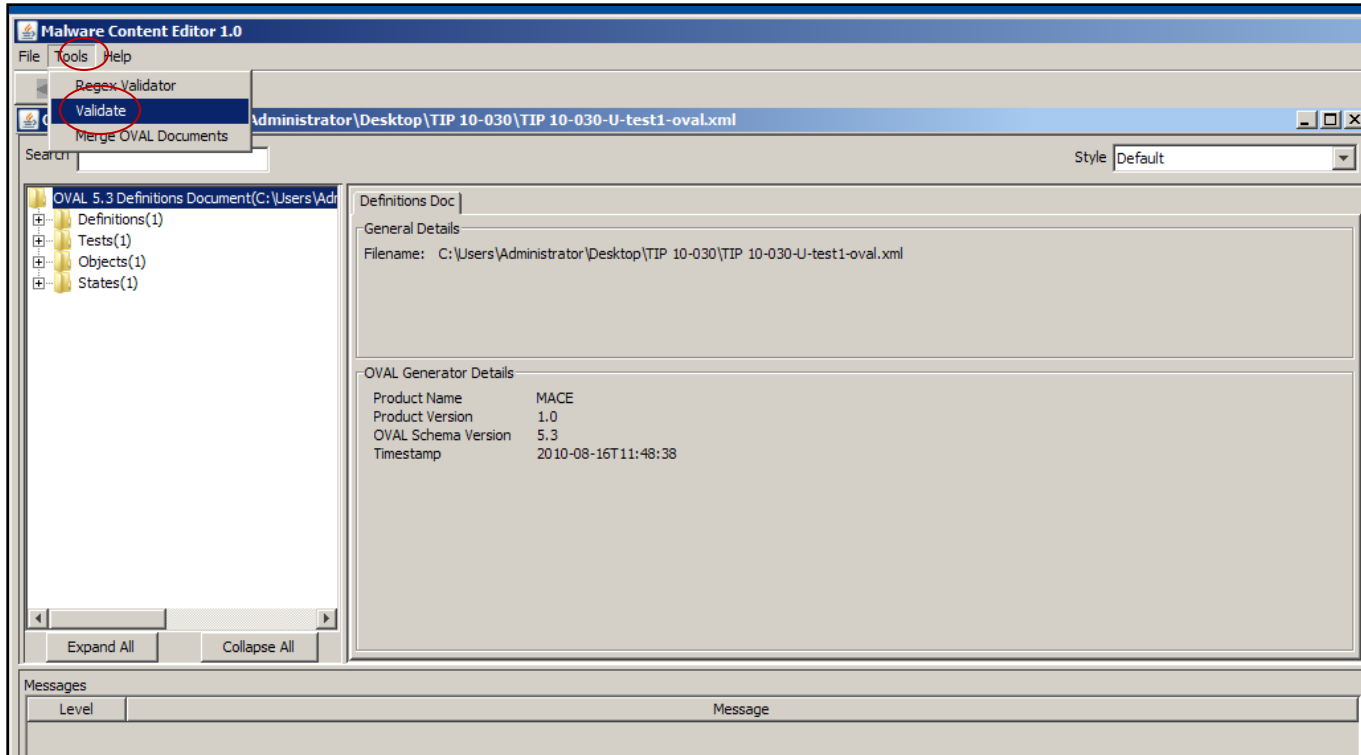
## PART 1



# OVAL Validation

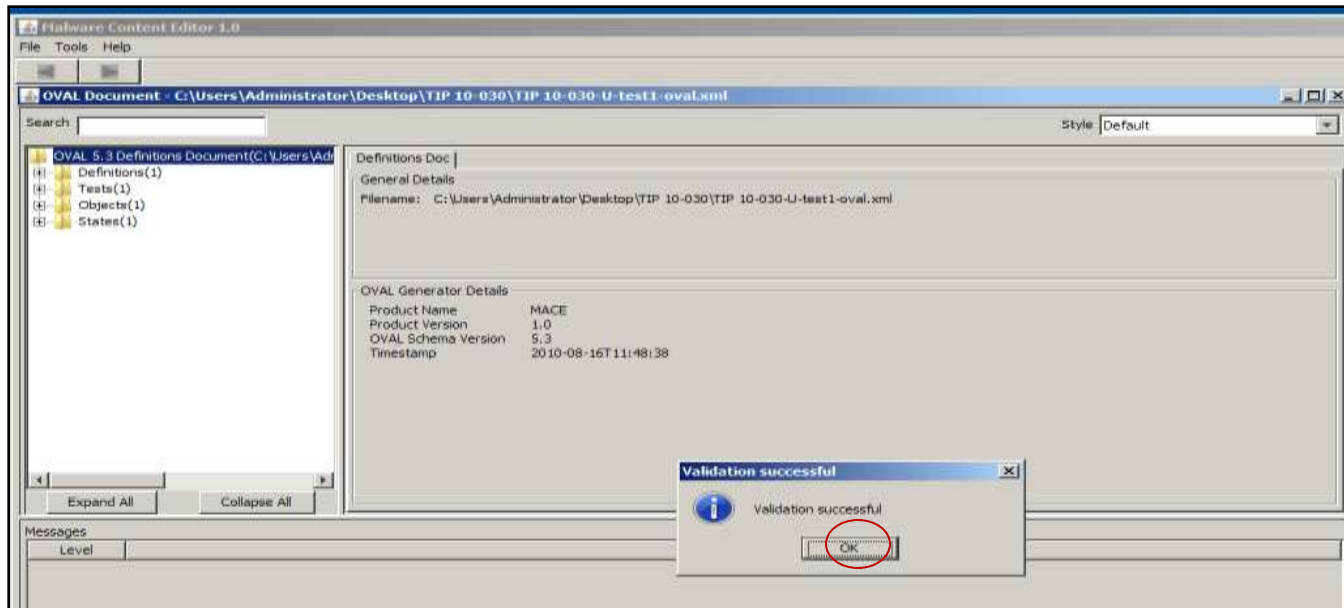


# OVAL Validation





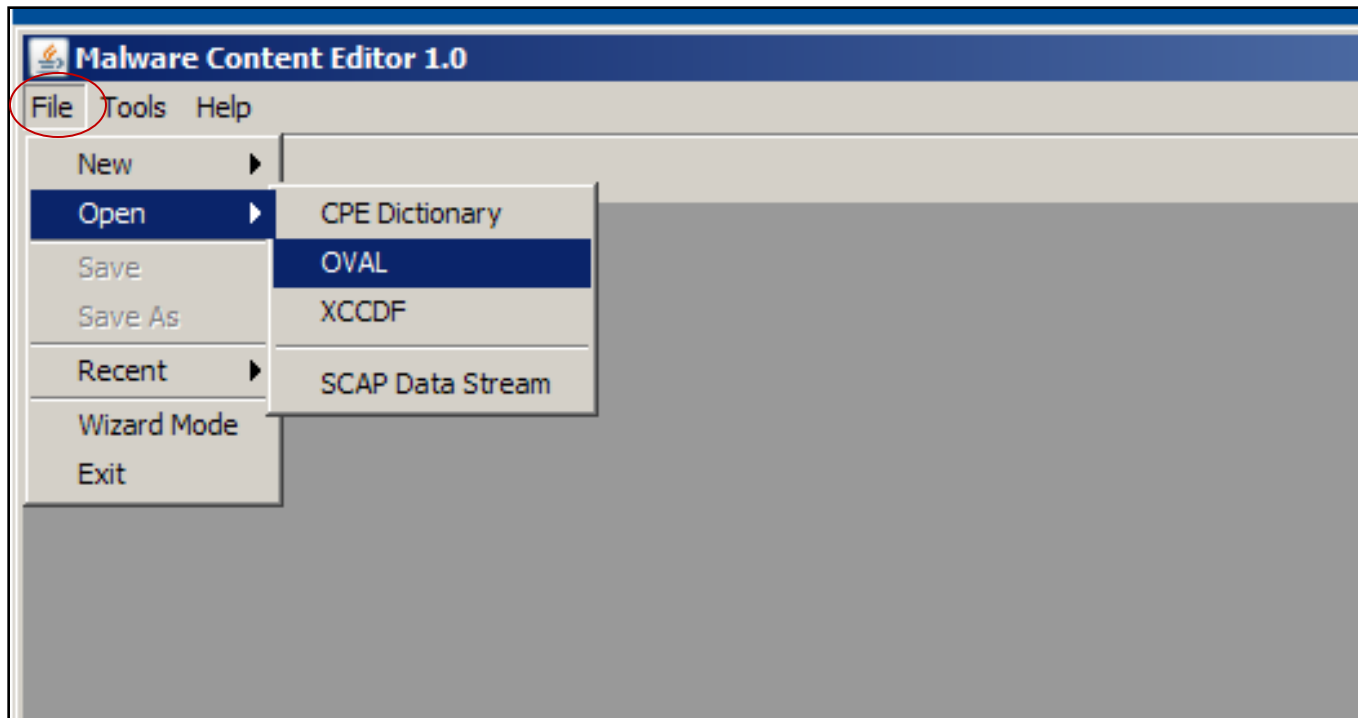
# OVAL Validation





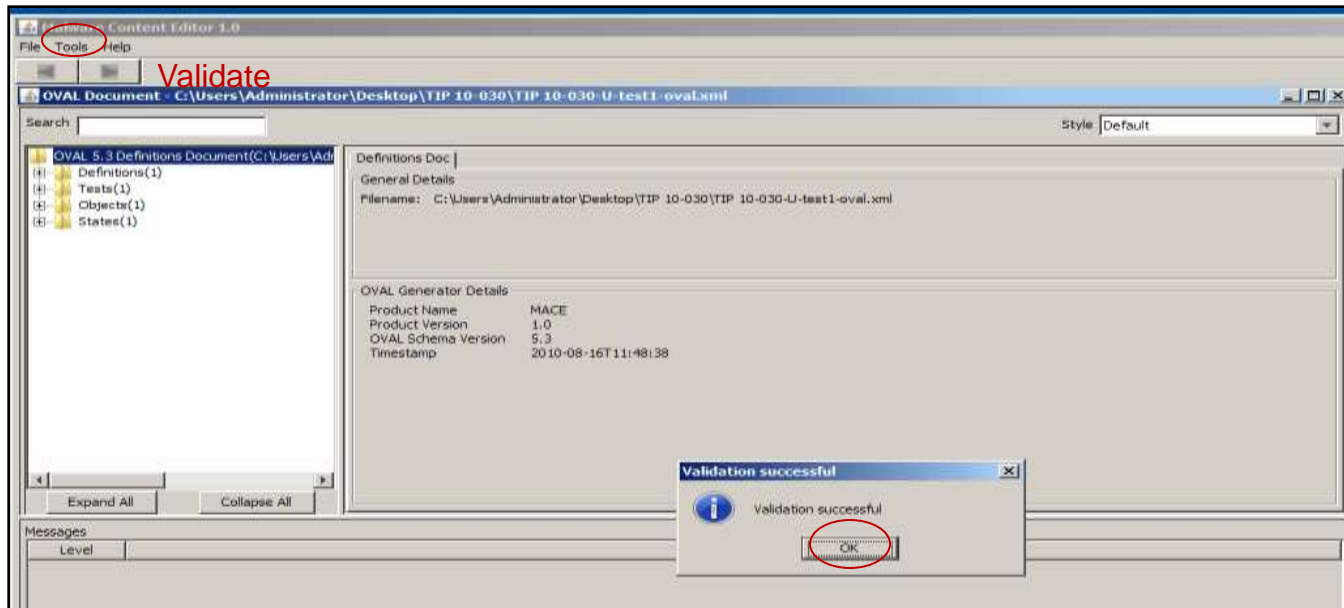


# OVAl Validation





# OVAL Validation





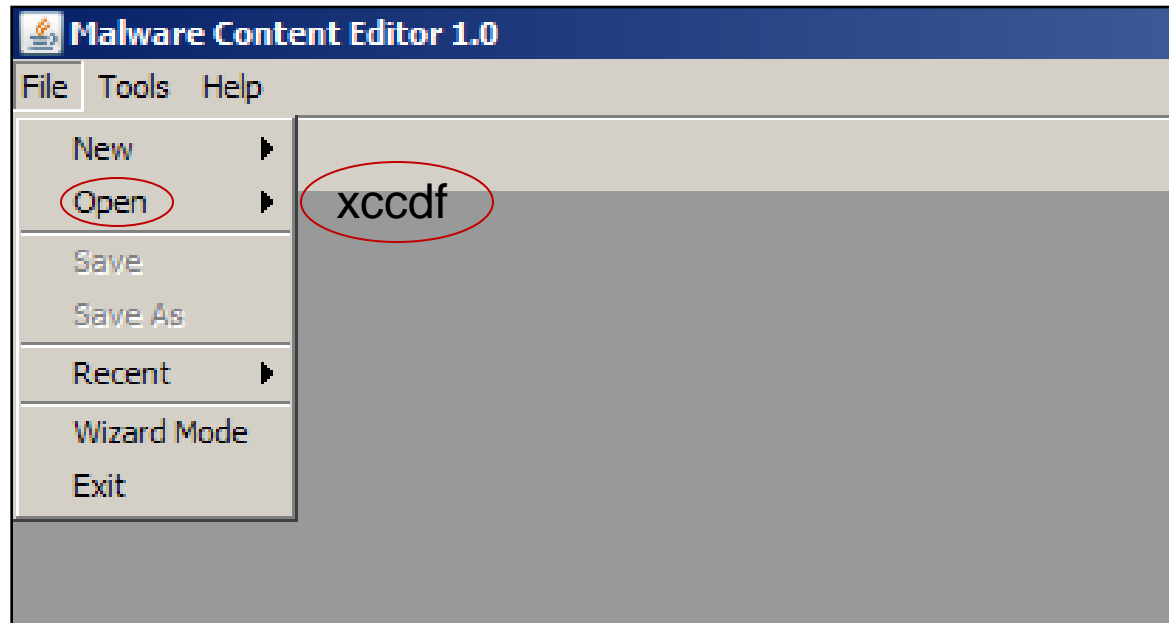
## PART 1



# Validate the Automatically Generated XCCDF

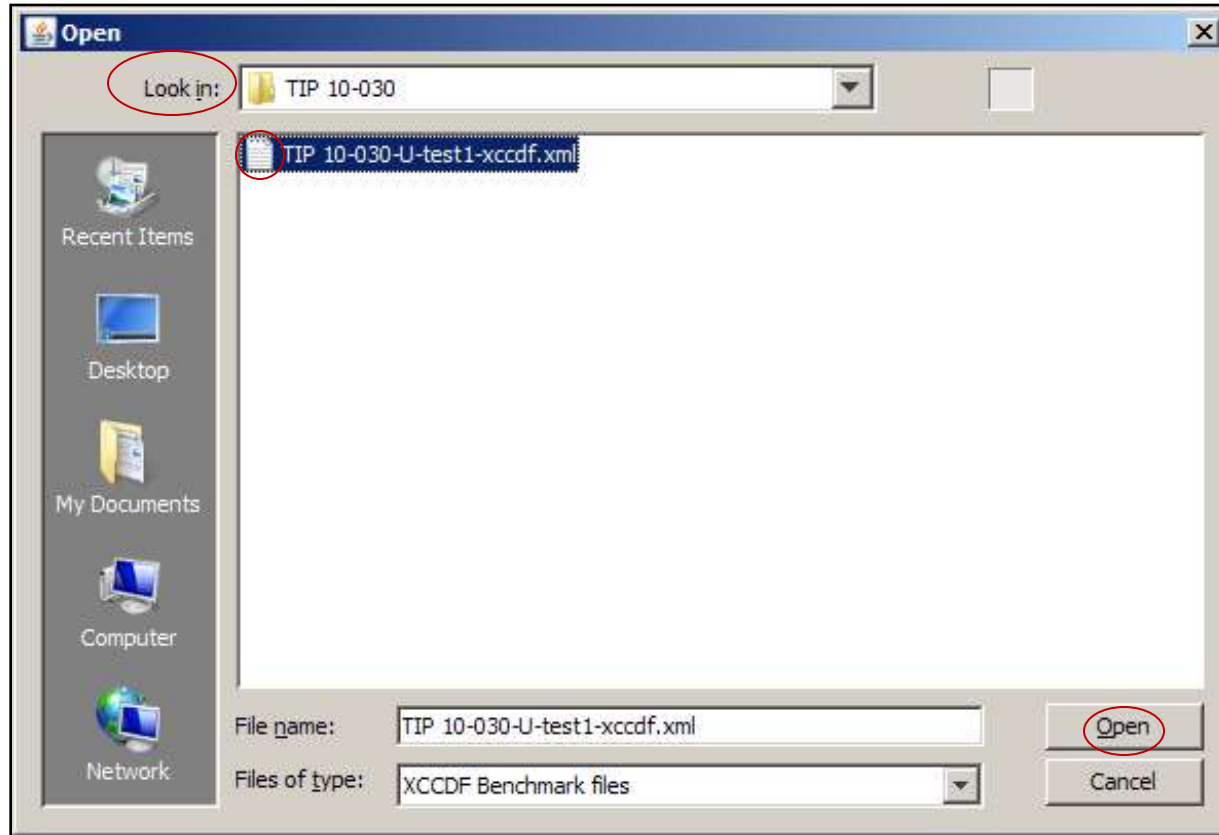


# XCCDF Validation



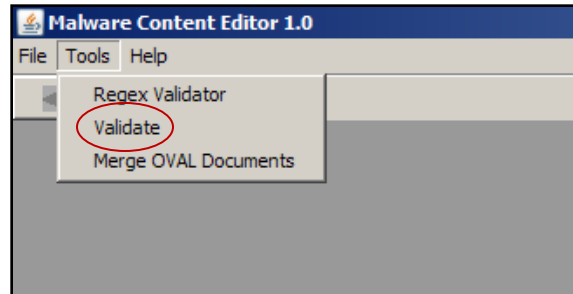


# XCCDF Validation





# XCCDF Validation





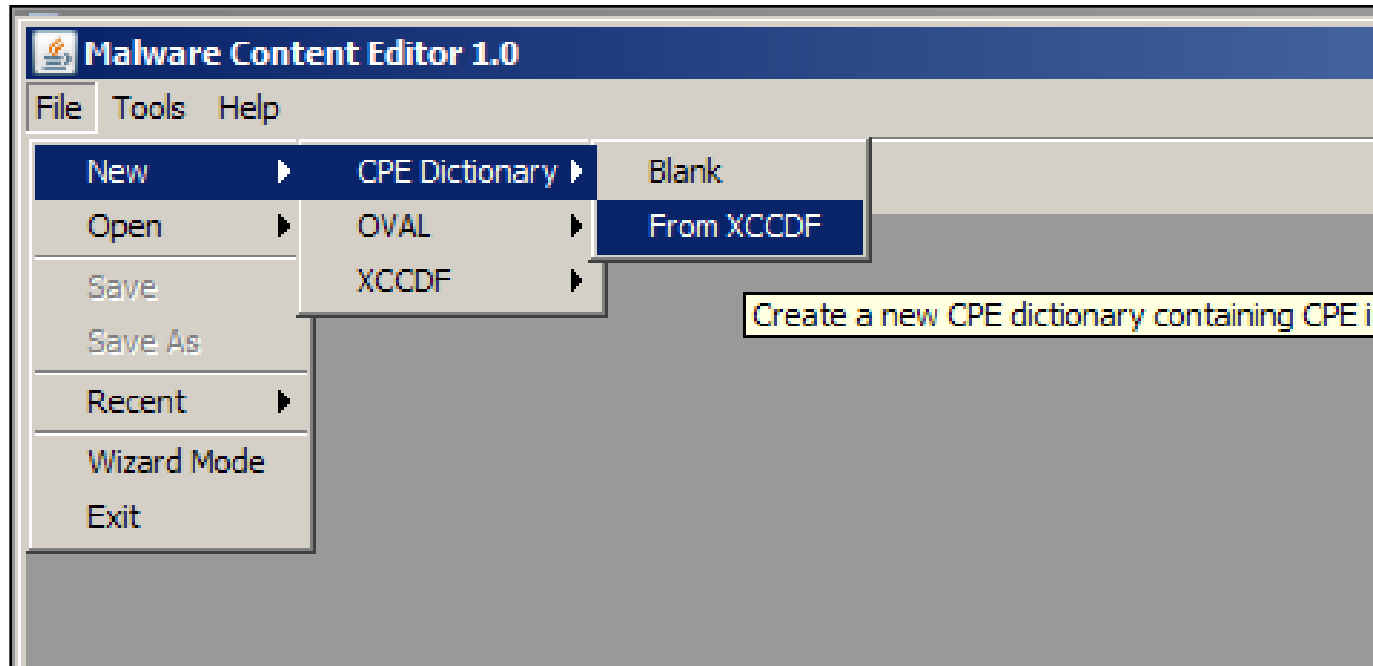
## PART 1



# Create Additional SCAP Data Stream files (from the XCCDF)



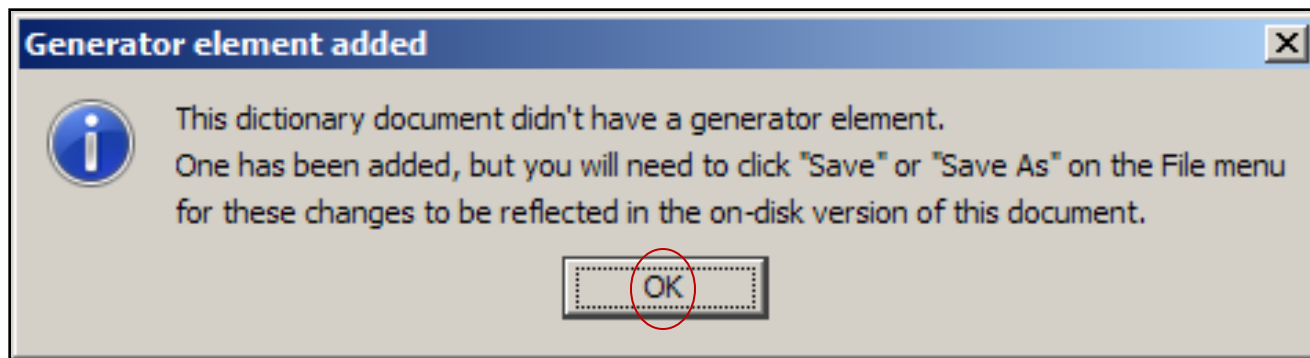
# Create the SCAP data stream files





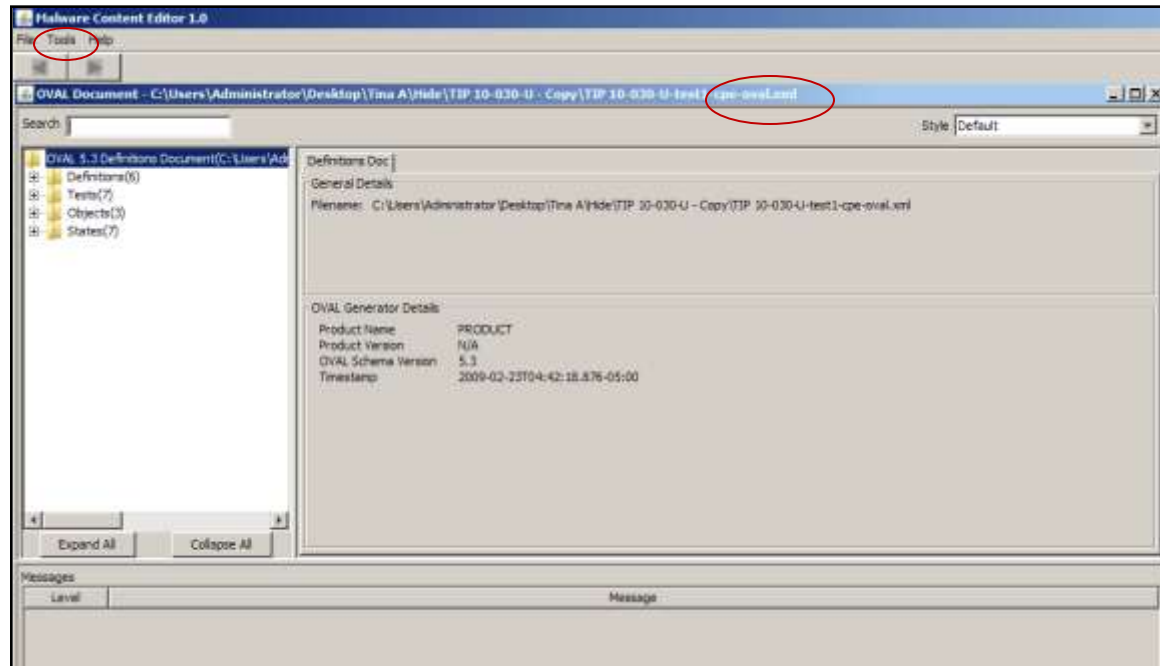


# Create the SCAP data stream files



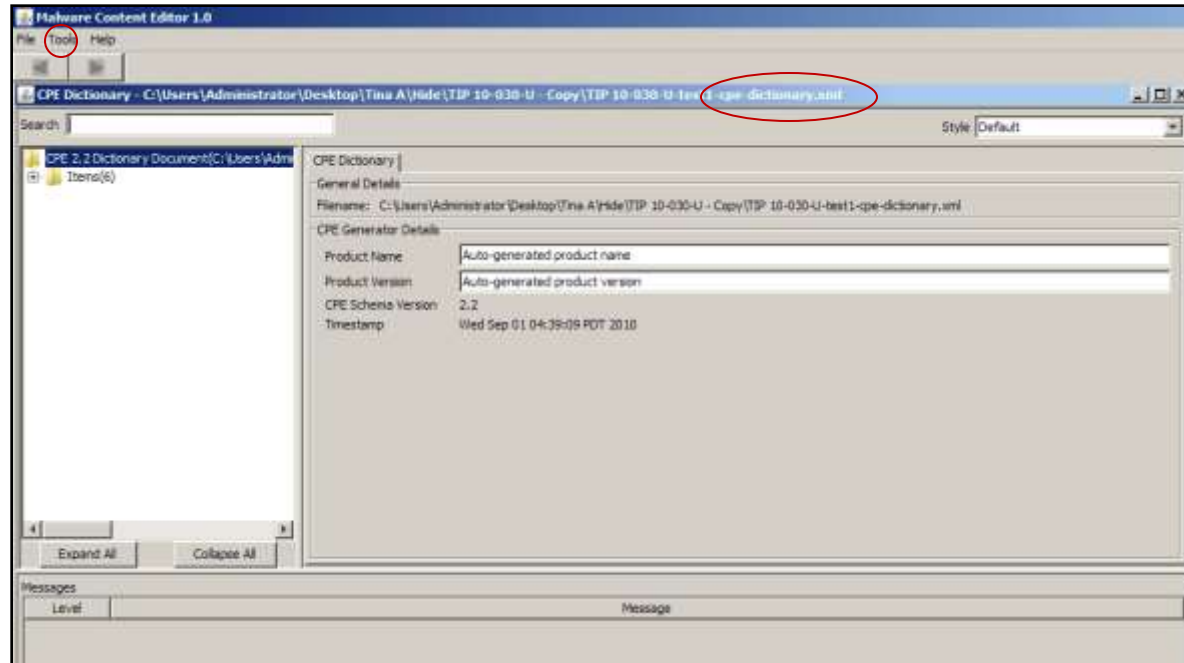


# Create the SCAP data stream files



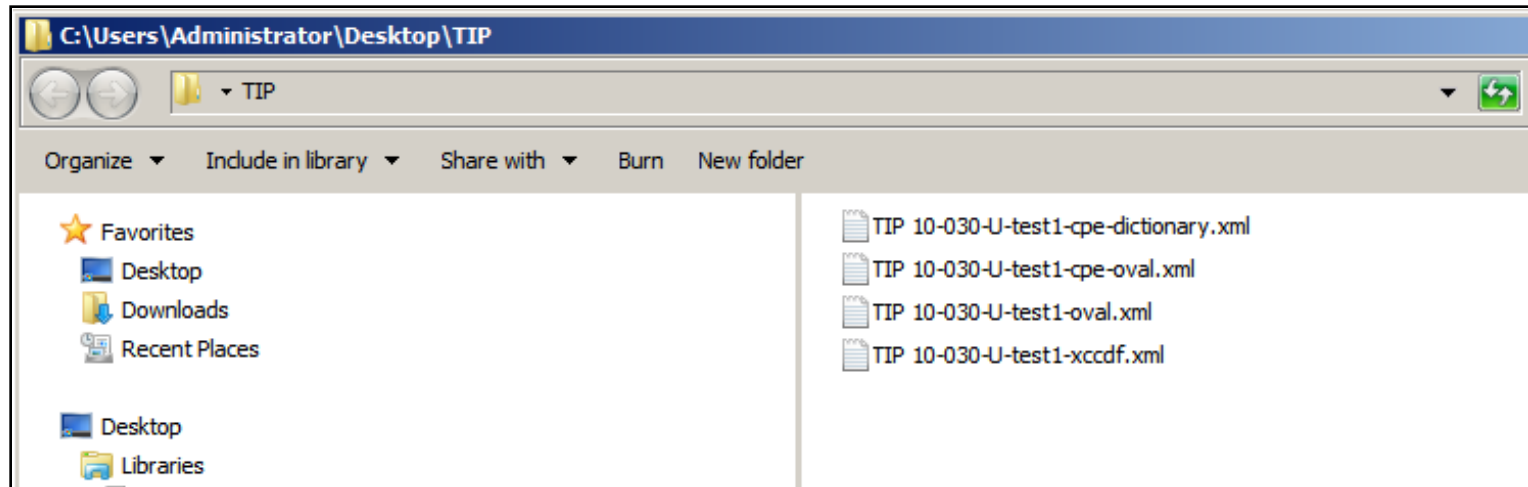


# Create the SCAP data stream files





# Create the SCAP data stream files

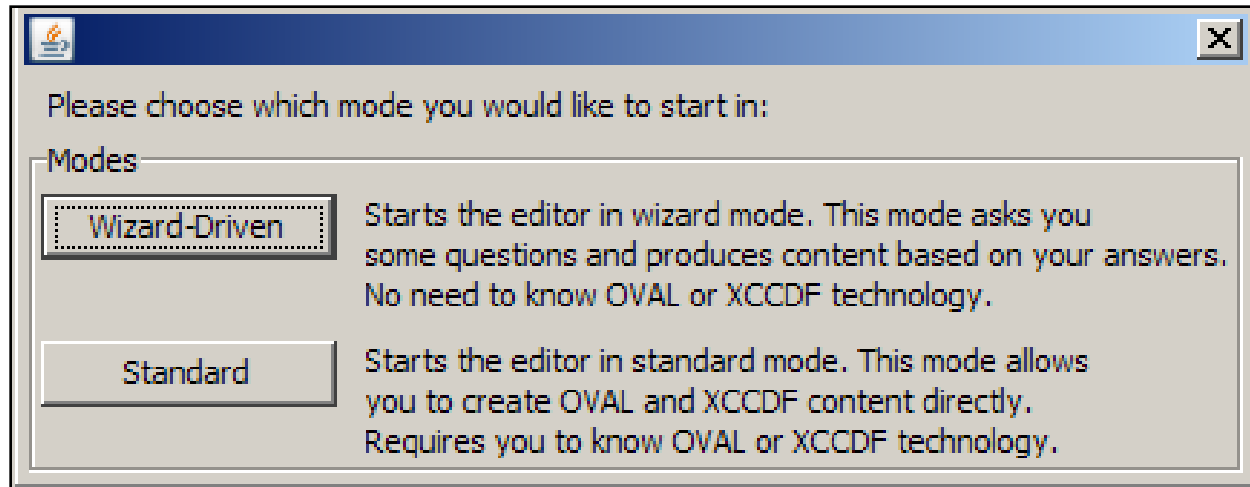




# PART 2



# OVAL Creation (for a registry entry)





# OVAL Creation (for a registry key)



**Malware Content Editor(Wizard Mode)**

Target OVAL version

1 OVAL\_53

OVAL Namespace Identifier

2 DOD.DIB.gov

What would you like to create?

3 File(windows) - Creates file/directory related content.  
File(unix) - Creates file/directory related content.  
Registry - Creates windows registry related content.

Go!



# OVAL Creation (for a registry key)



**Create new Registry Test**

Registry Hive/Key/Name

Title

What is to be tested

- Hive\Key exists - ignore Name and Value
- Hive\Key does NOT exist - ignore Name and Value
- Hive\Key\Name exists - ignore Value
- Hive\Key\Name does NOT exist - ignore Value
- Value of hive\key\name

Registry Hive

Registry Key  
  Regex

Registry Name  
Stub Path   Regex

Registry Value

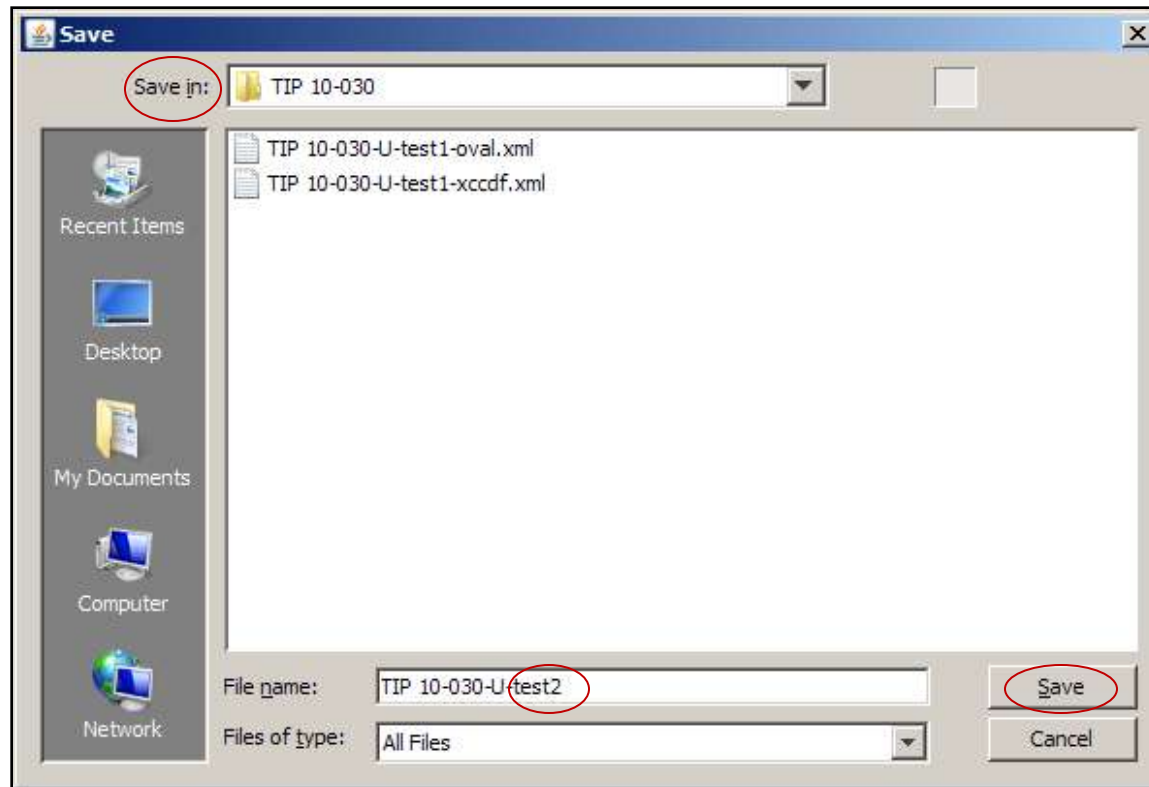
Datatype:  Operation:

Page 1 of 2





# OVAL Creation (for a registry key)





# OVAL Creation (for a registry key)



Malware Content Editor(Wizard Mode)

Target OVAL version  
OVAL\_53

OVAL Namespace Identifier  
DOD.DIB.gov

What would you like to create?

File(windows) - Creates file/directory related content.  
File(unix) - Creates file/directory related content.  
Registry - Creates windows registry related content.

Go!



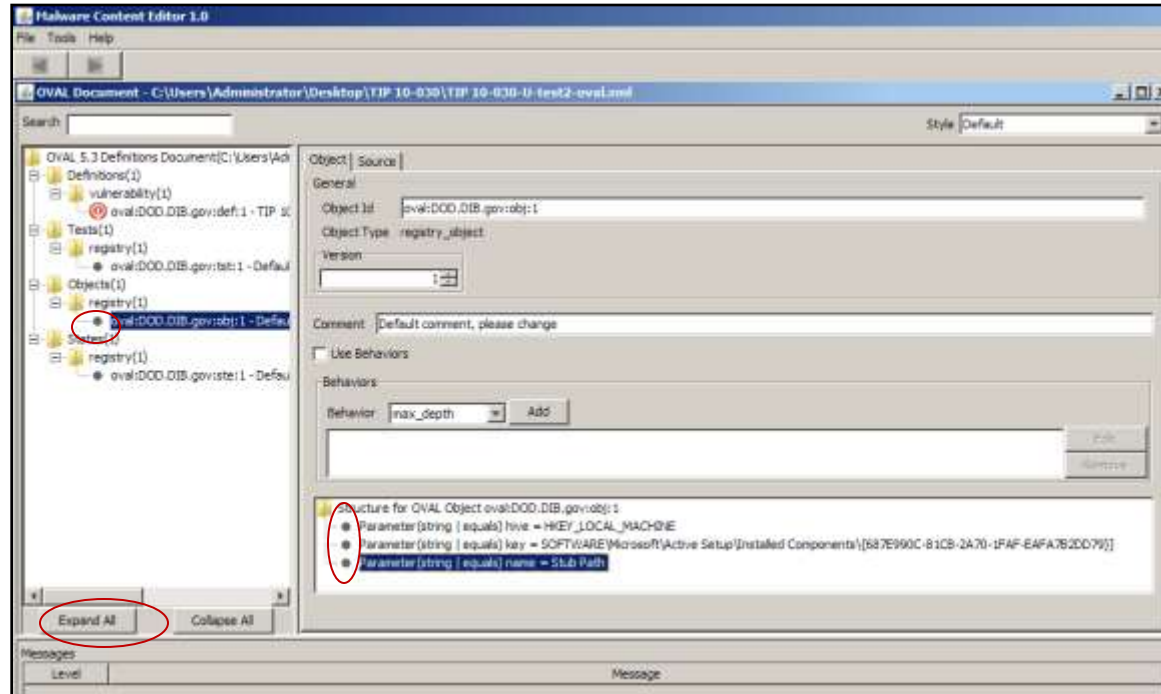
## PART 2



# OVAL Content Verification – Registry



# OVAL Content Verification – Registry





# OVAL Content Verification – Registry



Hardware Content Editor 1.0

OVAL Document - C:\Users\Administrator\Desktop\TIP 10-030\TIP 10-030-U-Test2-oval.xml

Search [ ] Style: Default

Definitions > vulnerability > ovals.DOD.DIB.gov:1 - TIP 11 > Tests > registry > ovals.DOD.DIB.gov:1 - Defau

State | Source |

General

State Id: oval.DOD.DIB.gov:state:1

State Type: registry\_state

Version: 1

Comment: Default comment, please change

Possible parameters

Parameter: hive [Add]

The hive that the registry key belongs to. This is restricted to a specific set of values: HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_CONFIG, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, and HKEY\_USERS.

Added parameters

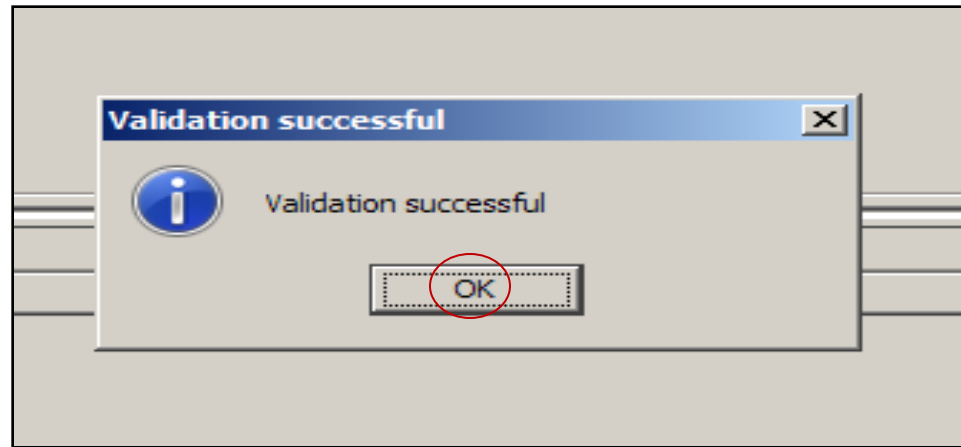
Name	Operation	Datatype	Value	Edit/Remove
value	equals	string	%System%\jast.exe	Edit/Remove

Messages

Level: Message



# OVAL Content Verification – Registry





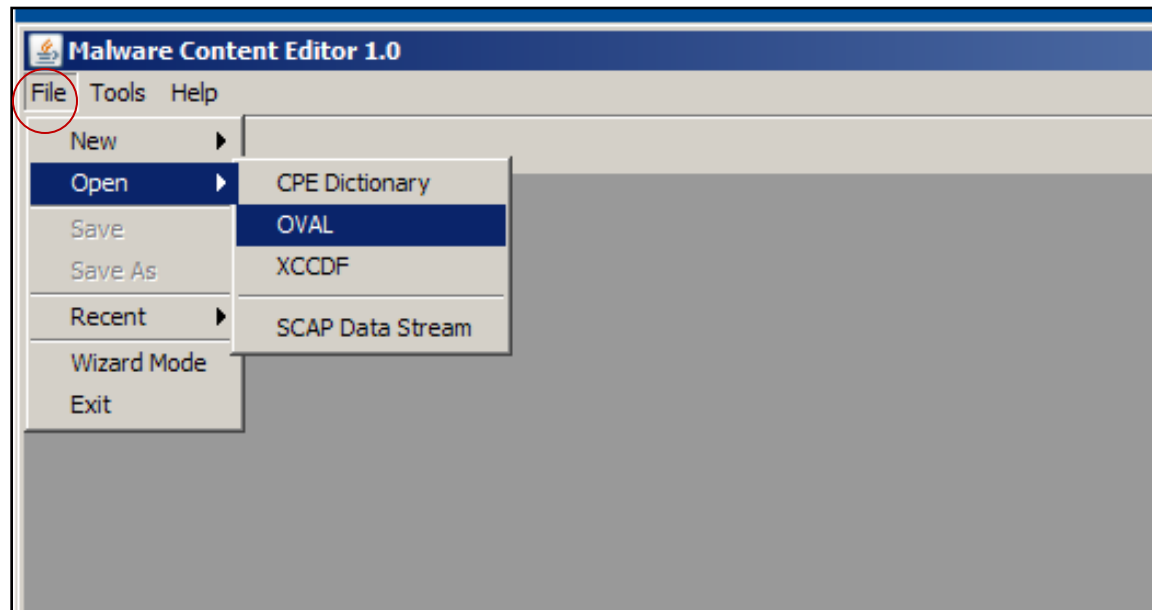
## PART 2



# Validate OVAL File



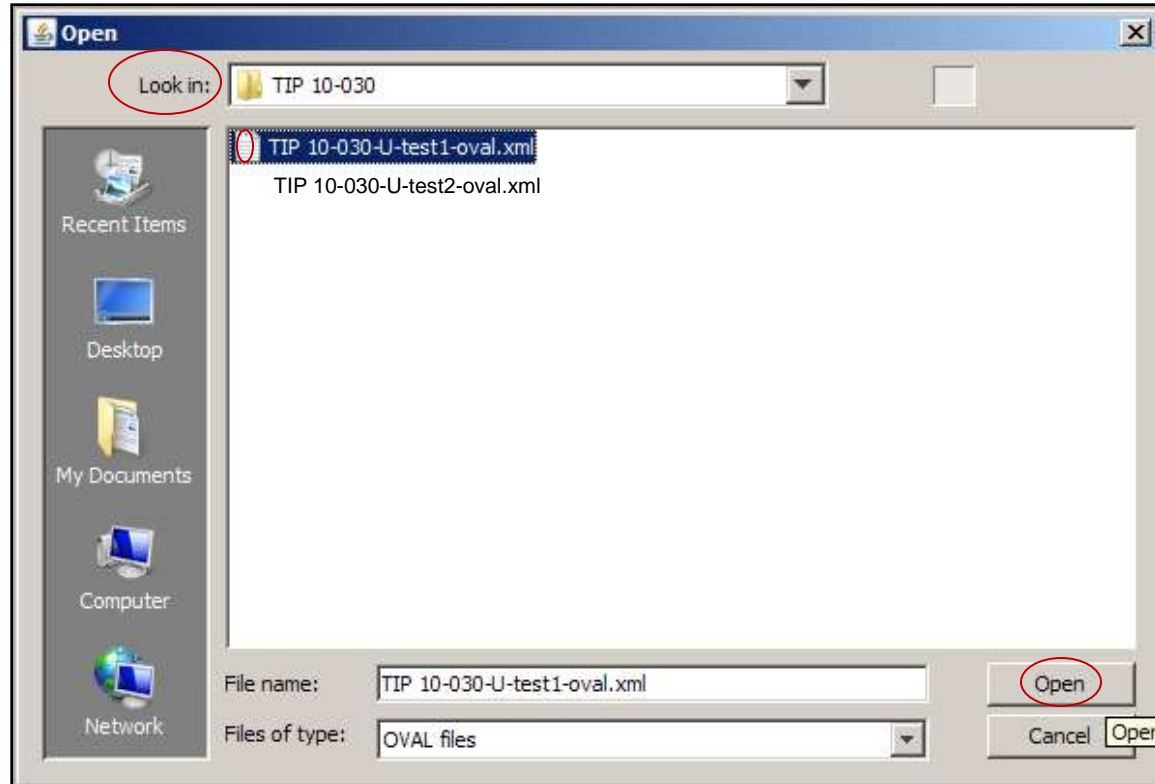
# Validate OVAL File





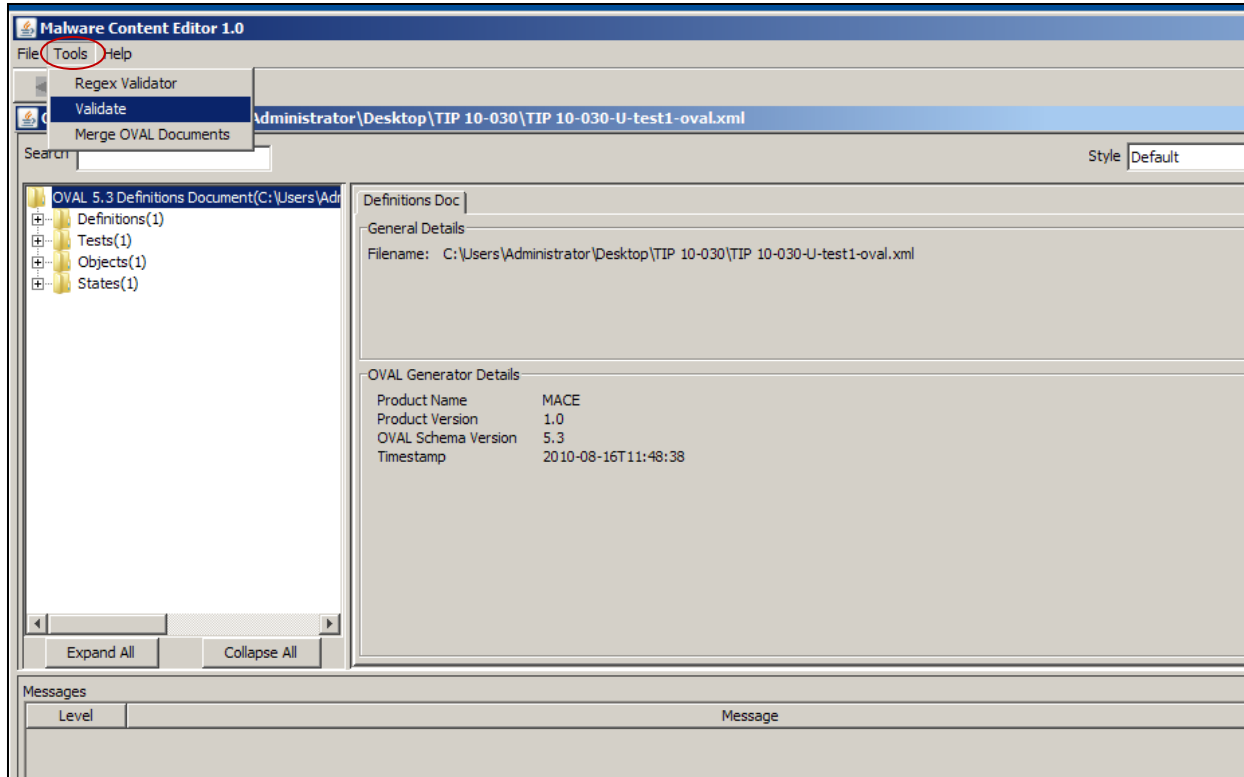


# Validate OVAL File



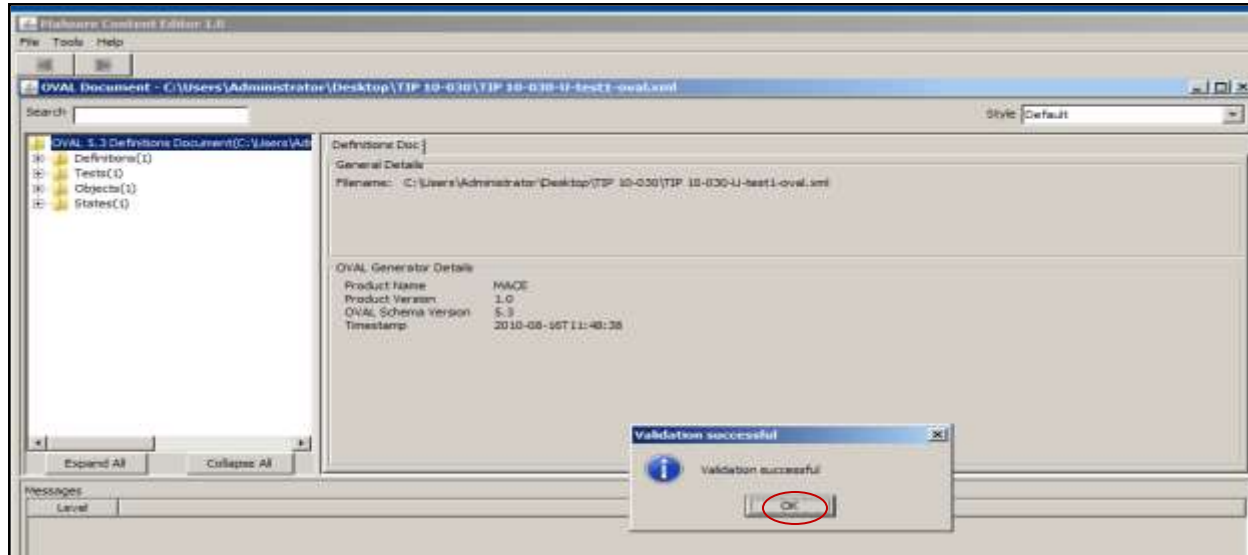


# Validate OVAL File





# Validate OVAL File





# OVAL Creation



**\*\*\*If you have additional registry checks then you will repeat these steps for all additional registry checks.**

**\*\*\*If you have additional OVAL Checks for files follow the steps in the previous section to generate, verify and validate each OVAL. Repeat these steps for any additional OVAL checks for files. The remaining slides will indicate how to merge all OVAL files and produce the FINAL OVAL.xml, FINAL-XCCDF.xml , FINAL-CPE-Dictionary.xml, and FINAL-CPE-OVAL.xml files**



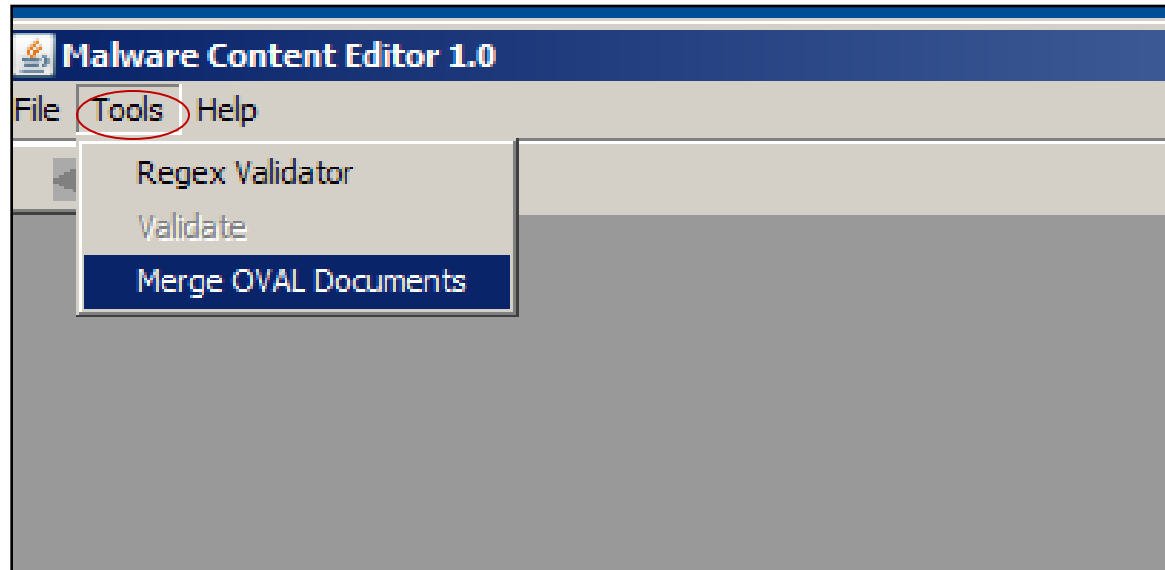
## PART 2



# Create FINAL-OVAL.xml by Merging Multiple OVAL files

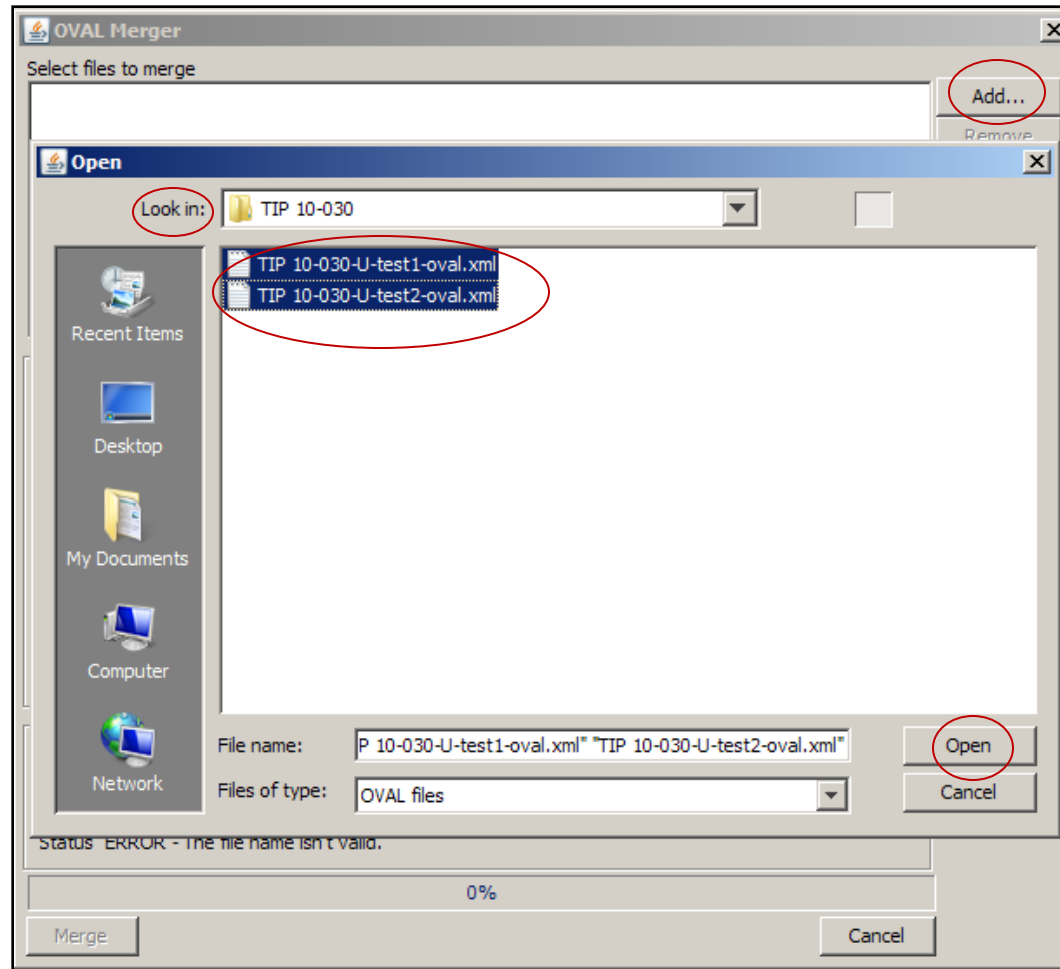


# Create FINAL-OVAL.xml by Merging Multiple OVAL files





# Create FINAL-OVAL.xml by Merging Multiple OVAL files

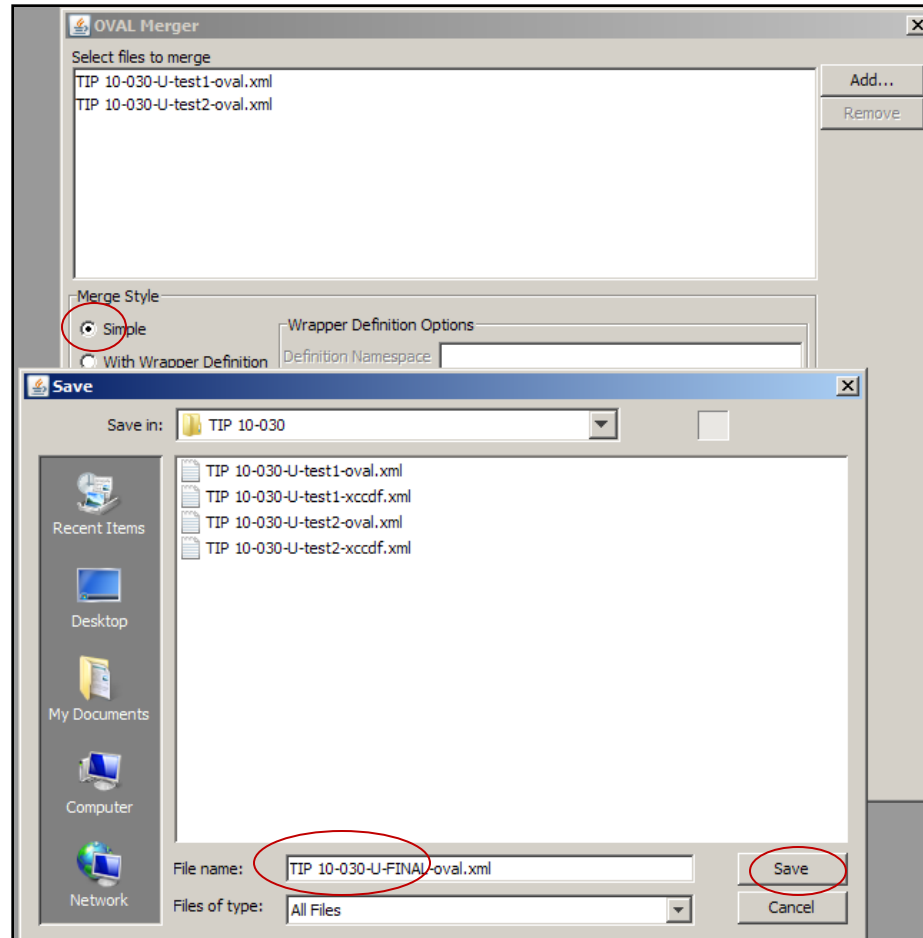




# Create FINAL-OVAL.xml by Merging Multiple OVAL files



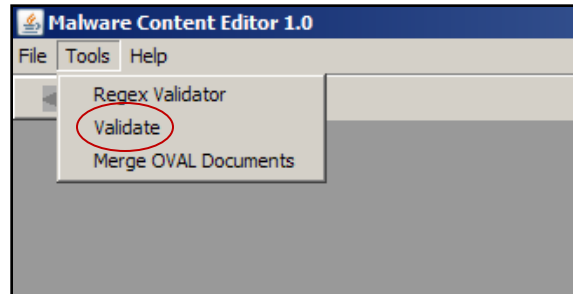
Select Browse  
& name FINAL







# Merged OVAL Validation





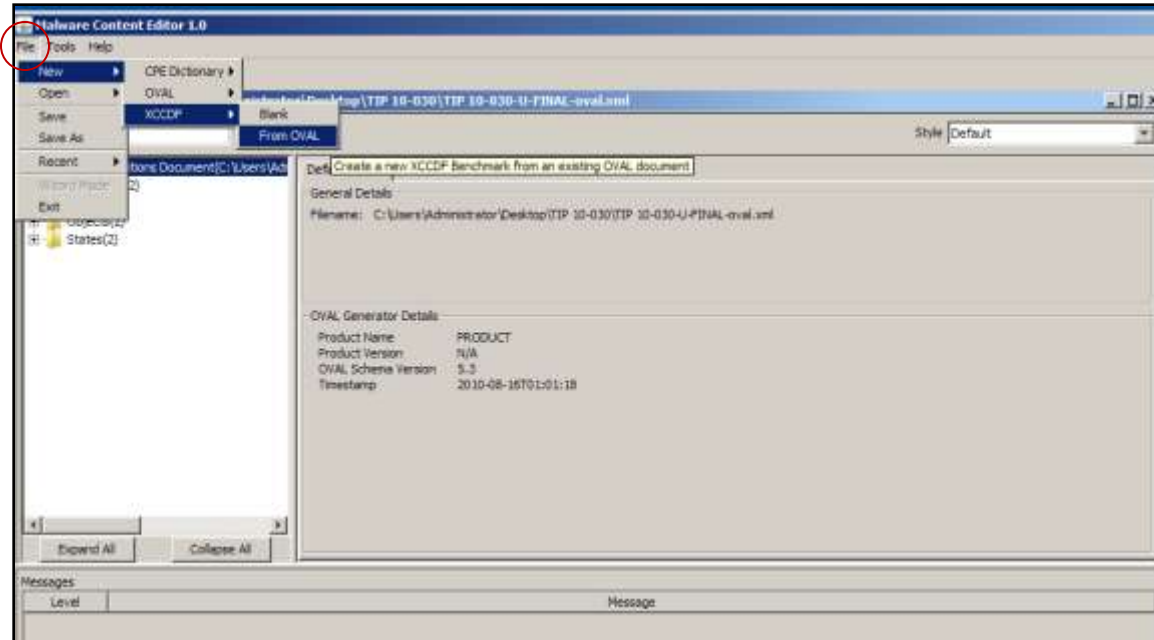
## PART 2



**Create the FINAL  
XCCDF.xml from the  
FINAL OVAL.xml**

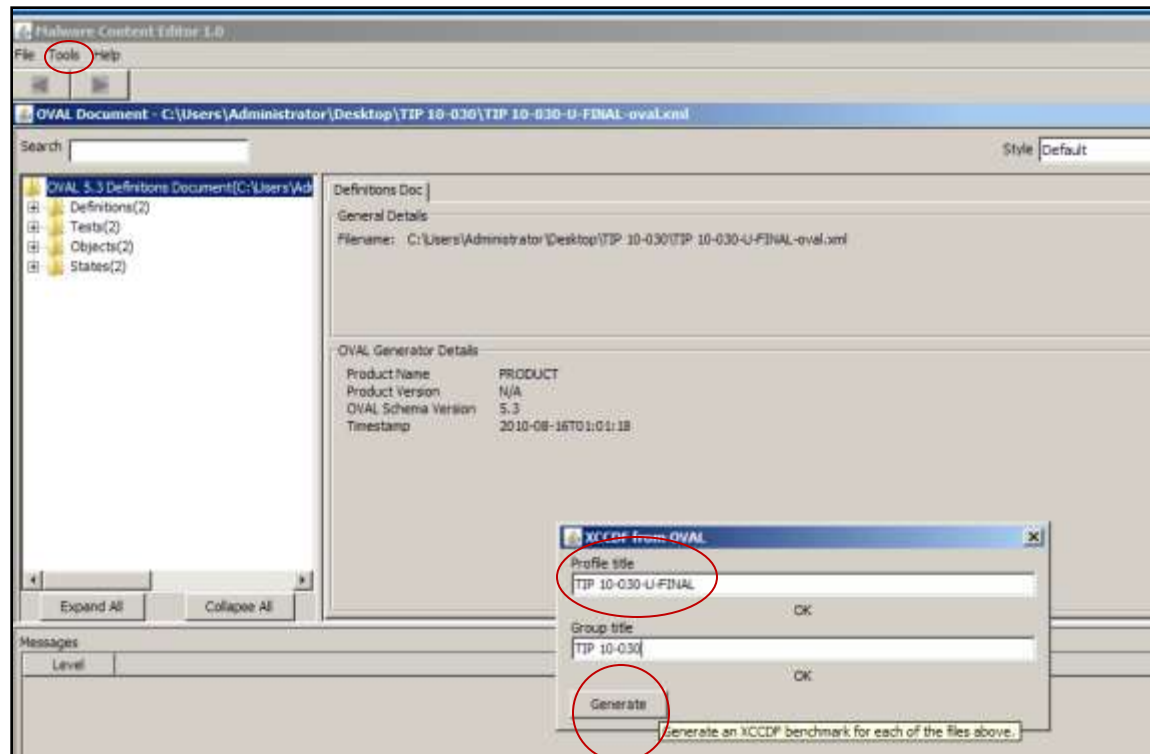


# Create the FINAL XCCDF.xml from the FINAL OVAL.xml



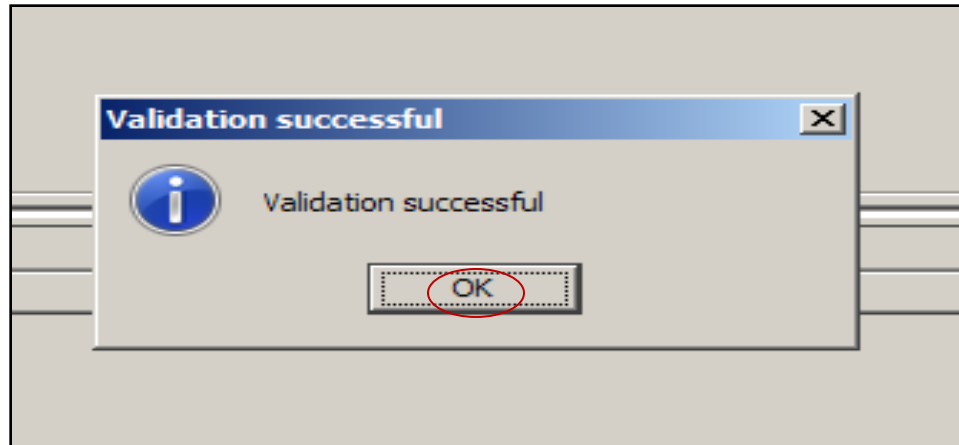


# Create the FINAL XCCDF.xml from the FINAL OVAL.xml





# Create the FINAL XCCDF.xml from the FINAL OVAL.xml





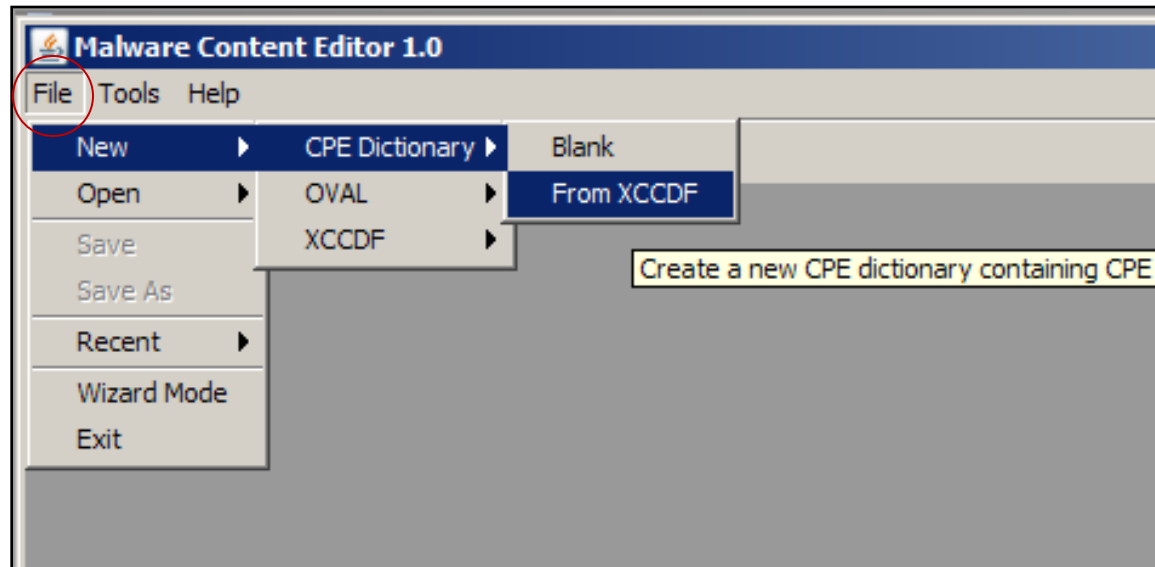
## PART 2



**Create the additional SCAP  
data stream files from the  
FINAL-XCCDF.xml**

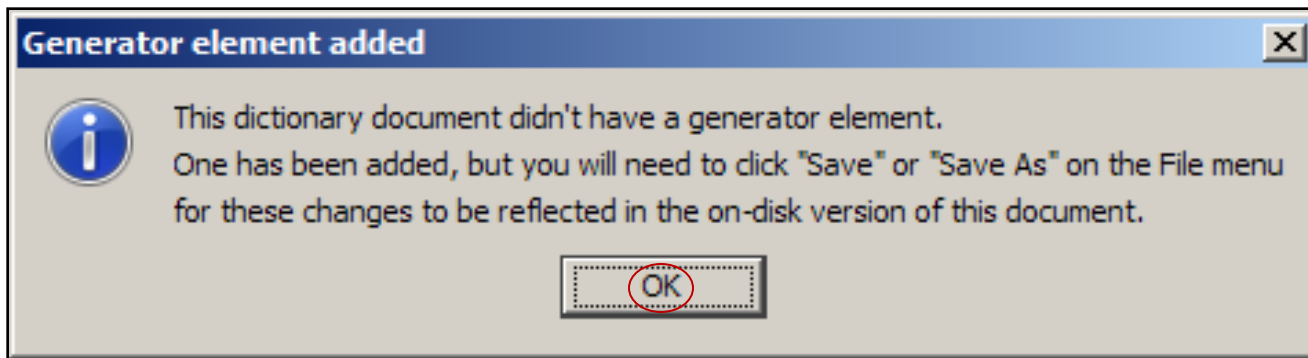


# Create SCAP data stream files from the FINAL-XCCDF.xml





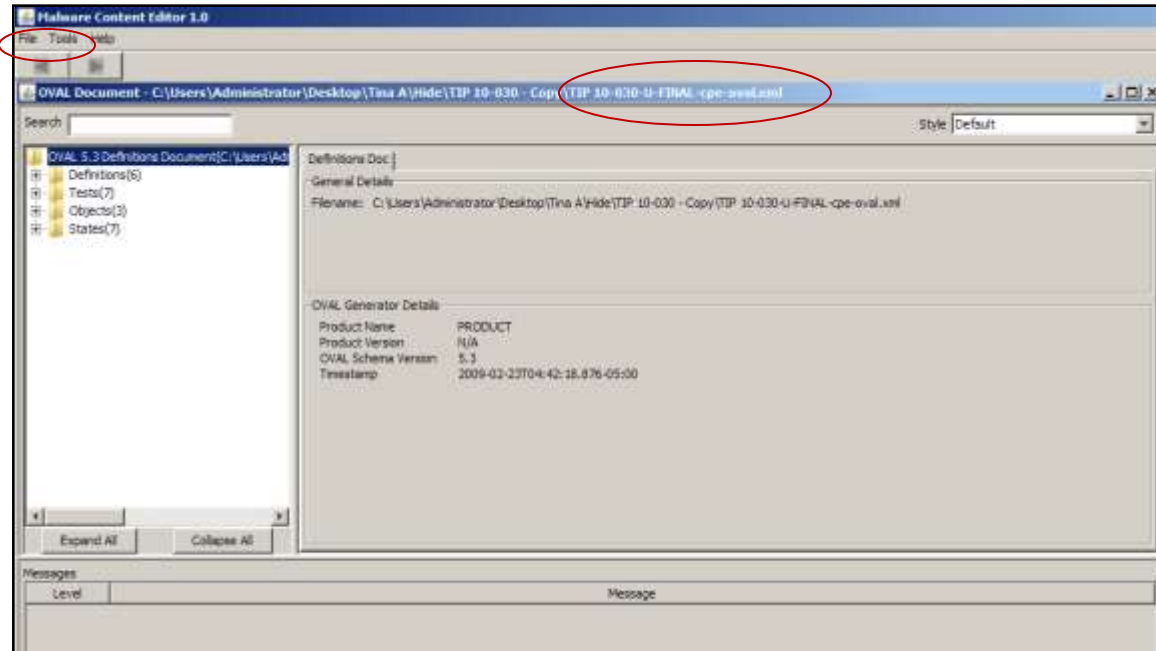
# Create SCAP data stream files from the FINAL-XCCDF.xml







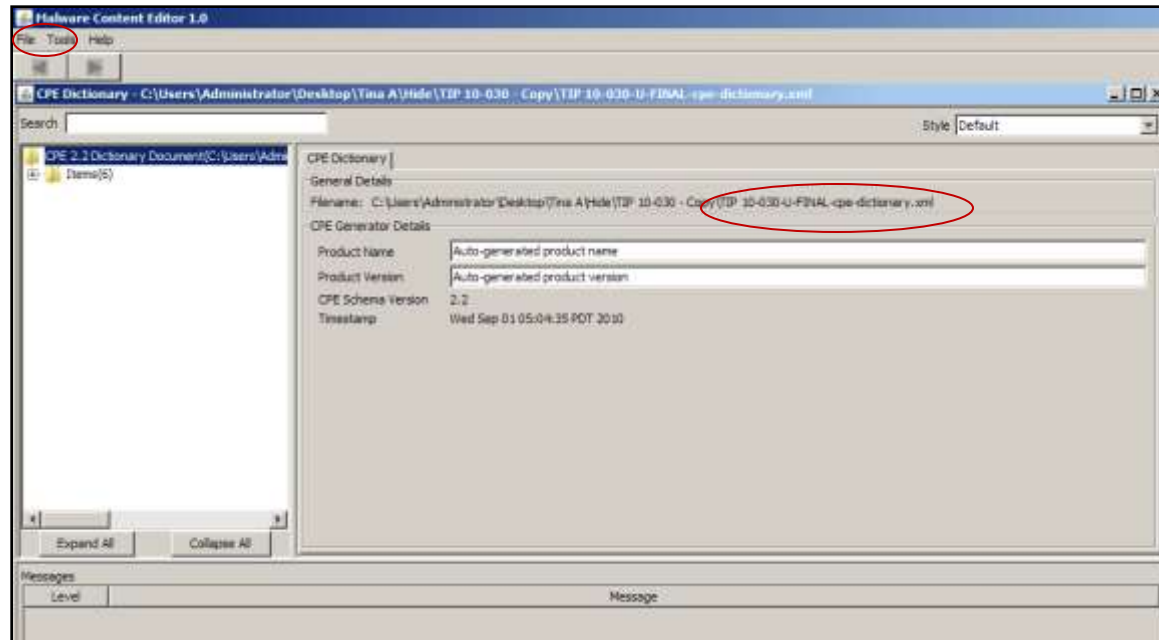
# Create SCAP data stream files from the FINAL-XCCDF.xml



**File > Save > Tools > Validate > Close xml**



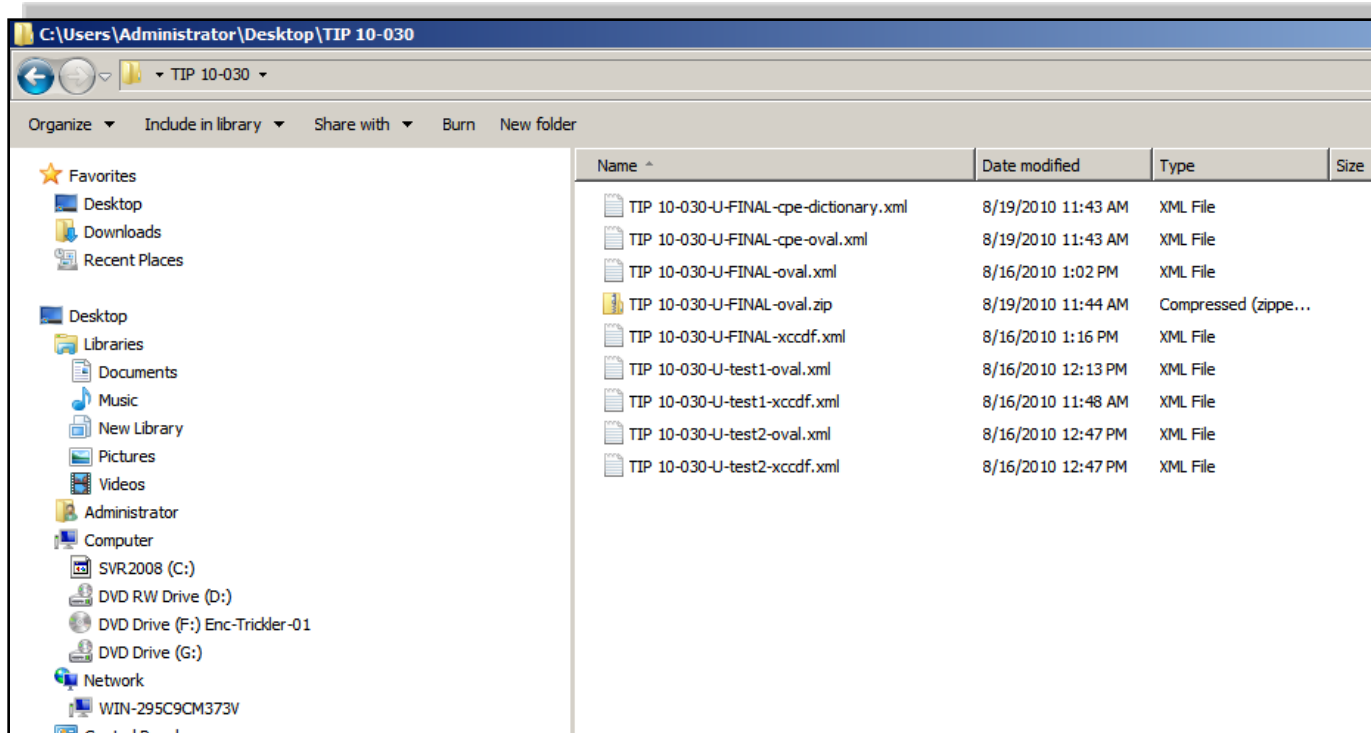
# Create SCAP data stream files from the FINAL-XCCDF.xml



**File > Save > Tools > Validate > Close xml**



# Create SCAP data stream files from the FINAL-XCCDF.xml



**View Folder**



?????'s



# POC's



- **Tina Ackerman, DoD**  
**410-854-0692**
  
- **Mike Kinney, DoD**  
**m.kinne@radium.ncsc.mil**
  
- **Shane Shaffer, G2**  
**shane.shaffer@g2-inc.com**  
**s.shaffe@radium.ncsc.mil**



**THE DECISIVE ADVANTAGE**