# **Open source scan**

Table of Contents

[Open source scan 1](#_Toc481015948)

[1. License 2](#_Toc481015949)

[2. Blackduck install and configuration 3](#_Toc481015950)

[2.1 About blackduck 3](#_Toc481015951)

[Open Source Compliance & Management 3](#_Toc481015952)

[2.2 Blackduck for Cisco 5](#_Toc481015953)

[2.3 Download Blackduck 6](#_Toc481015954)

[2.4. install Blackduck 7](#_Toc481015955)

[2.5 Configuration for local scan client 8](#_Toc481015956)

[3. Scan code with Blackduck tool 9](#_Toc481015957)

[3.1 Create scan project 9](#_Toc481015958)

[3.2. Analysis project code 11](#_Toc481015959)

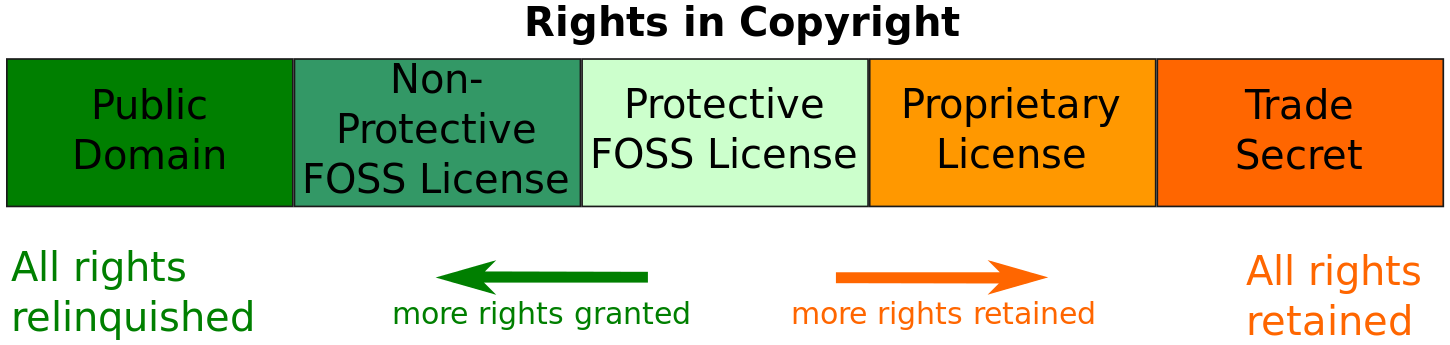
[4. Check Analysis result 13](#_Toc481015960)

[4.2 Analysis result for match code 15](#_Toc481015961)

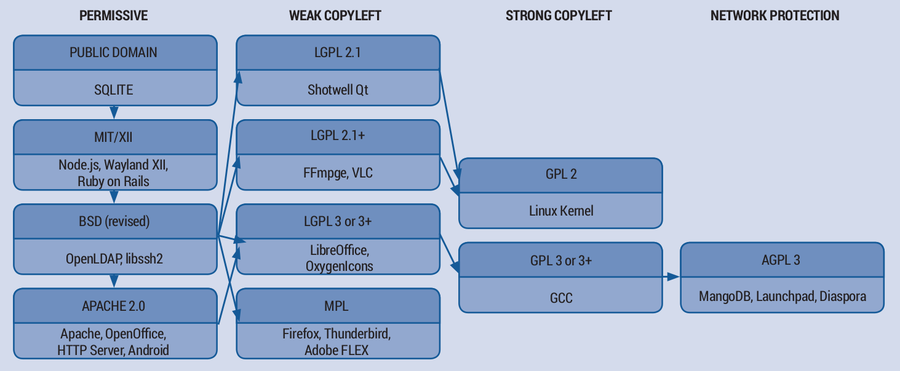
# **License**

## **1.1 Free software license**

WIKI: <https://en.wikipedia.org/wiki/Free_software_license>



## **1.2 License**



* GPL

<https://en.wikipedia.org/wiki/GNU_General_Public_License>

* LGPL
* BSD
* MIT
* Appache
* others

# **Blackduck install and configuration**

## **2.1 About blackduck**

**website:**

Blackduck office website: <https://www.blackducksoftware.com/>

Blackduck product and solution: <https://www.blackducksoftware.com/about>

Compliance: <https://www.blackducksoftware.com/solutions/open-source-license-compliance>

Security: <https://www.blackducksoftware.com/solutions/application-security>

**Product/solution:**

# **Open Source Compliance & Management**

Black Duck® [Protex](https://www.blackducksoftware.com/products/protex)™ integrates with existing development tools to automatically scan your code and identify software origins to reduce business risks.

* Open source identify

Scan and check which third-party open source code in your project

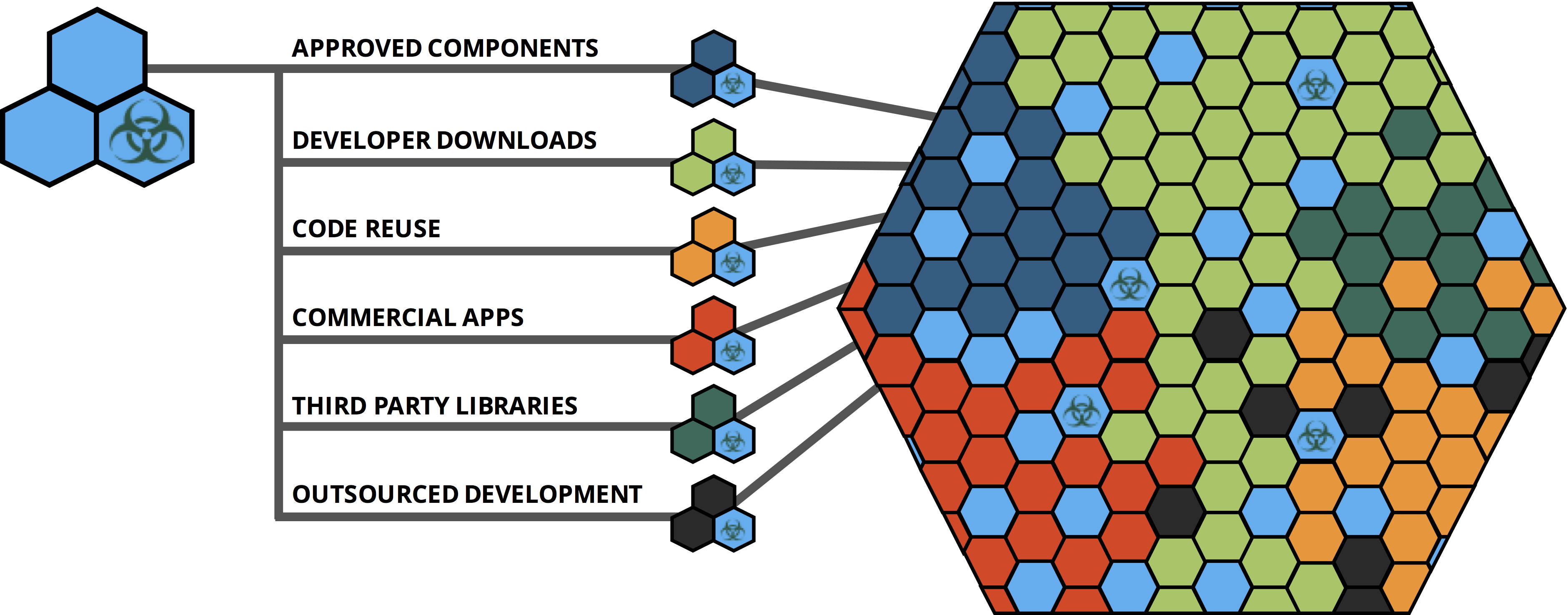
* Open source license compliance

Check which license those open source you are using

GPL? LGP? BSD? etc.

* Which open source can be reused based on company policy/audit
* Provide a license obligation report

**Security**



* What open source components are in your code?
* Are they affected by known security vulnerabilities?
* Are they up-to-date and do they comply with policy?

**Security solution**

* Identifies open source throughout your code base
* Automatically maps open source in use to known open source security vulnerabilities
* Flags policy violations and tracks remediation progress
* Continuously monitors for newly identified open source vulnerabilities

## **2.2 Blackduck for Cisco**

**Login:**

both local and online, login with **CEC ID**

**Support team mail list:**

If you failed to login blackduck website via CEC ID, please ask support team for help

Firstly, contact with:

John Smarrella-X [jsmarrel@cisco.com](mailto:jsmarrel@cisco.com)

or below mail list:

Srikanth Malipatlolla -T (srmalipa - COMPUCOM SYSTEMS INC at Cisco) <srmalipa@cisco.com>;

Adibettahalli Anand (aanand) <aanand@cisco.com>;

ABHINEET DESHPANDE (abhindes) <abhindes@cisco.com>;

Allan Dolores -X (adolores - TECHNICOLOR SA at Cisco) <adolores@cisco.com>;

Sandeep Mehta (sandemeh) [sandemeh@cisco.com](mailto:sandemeh@cisco.com)

**online scan result:**

<http://sjc-ipaudit-1/protex/ProtexLoginPage?uifsid=2#0=dW,dx,gc,gL,fI,cS>

**local scan via client:**

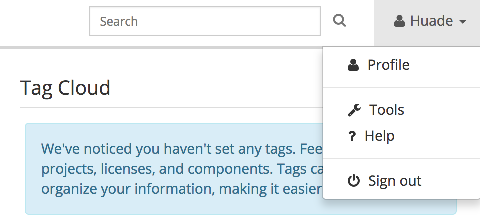
http://localhost:9000

for how to scan with local client, please refer to 2.3 for installation and 3 for code scanning

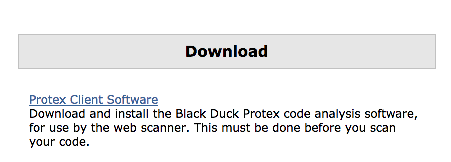
## **2.3 Download Blackduck**

**Step 1**. Go to <http://sjc-ipaudit-1/p/dashboard> and login with your **CEC ID**

**Step 2.** Go to **Tools** page, as show below, click Tools



**Step 3.** Then click [**Protex Client Software**](http://localhost:9000/protex/ProtexIPToolsClientSoftwareContainer?uifsid=1) as show below



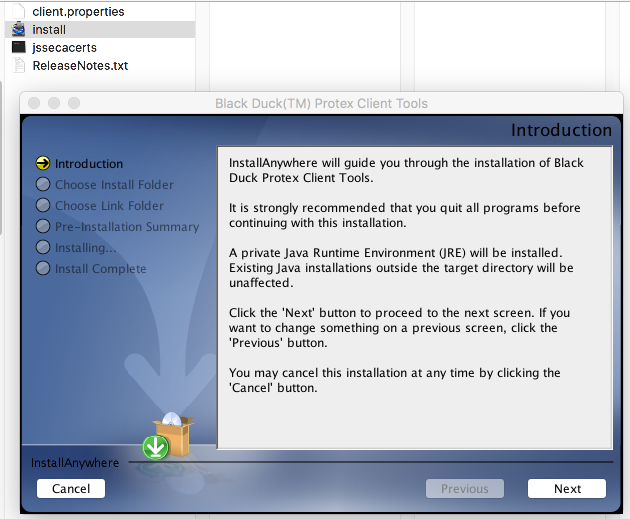
**Step 4:** Download **protex client** version based on your actual os, like Mac etc.



## **2.4. install Blackduck**

After download, click install file to install **protex client**.

Below shows the installation on mac



## **2.5 Configuration for local scan client**

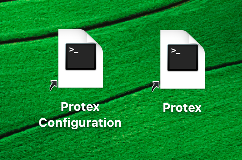
After installation, there will be tow command line short cut for protex client

* **Protex Configuration**

Need to configure your local protex client’s servers URL

* **Protex**

Local client for code scanning



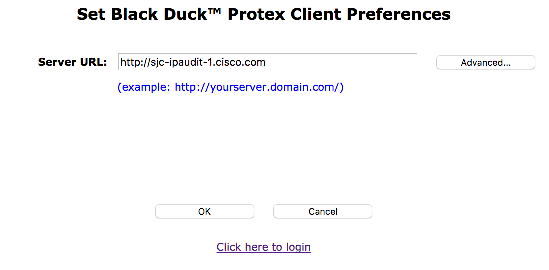
**Step 1,** click **Protex Configuration** for server URL setting

Will direct to below web page for URL setting

<http://localhost:9000/client/setPrefs.jsp>

**Step 2,** setting server URL for **Protex**

<http://sjc-ipaudit-1.cisco.com> is preferences setting

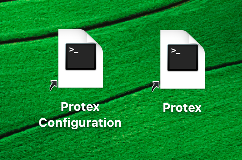


# **Scan code with Blackduck tool**

## **Create scan project**

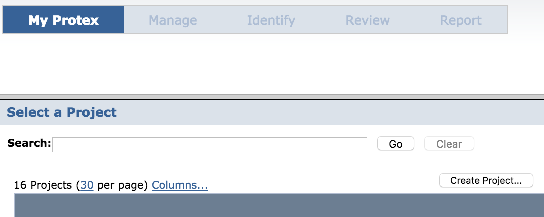
**Step 1,** click Pretex client command tools as below(On Mac)

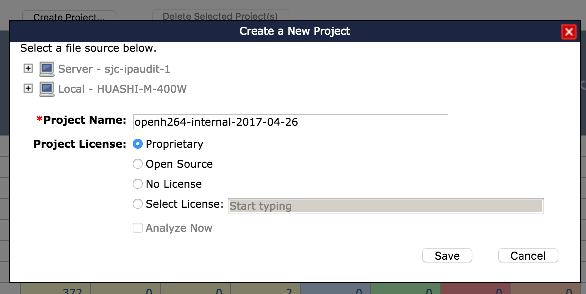
Will direct to page <http://localhost:9000/protex/?uifsid=3#0=dW,dx,gc,gL,fI>



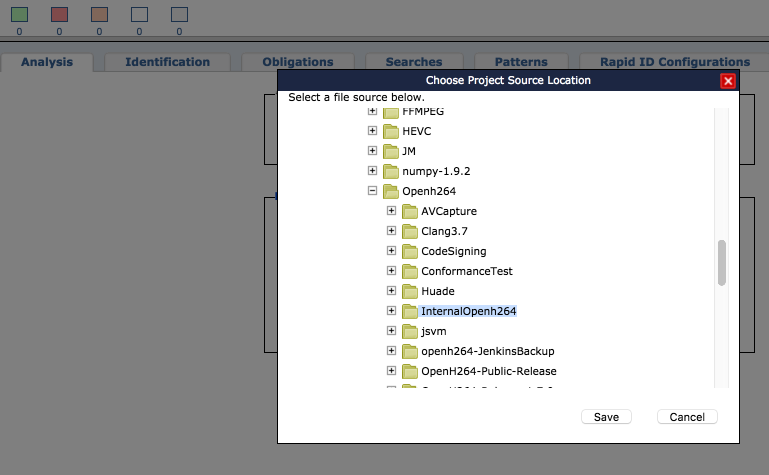
**Step 2;** Click Create Project to create one project for code scanning

Below shows create one openh264-internal-2017-04-26 project to scan latest internal openh264’s project code



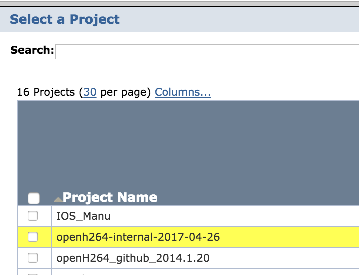


**Step 3,** Choose local code location and then click save



## **3.2. Analysis project code**

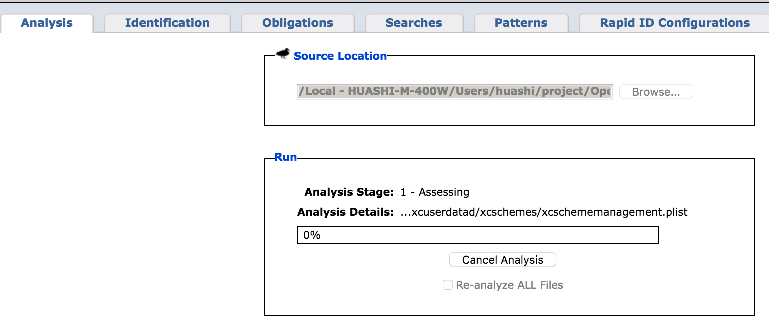
**Step 1**, Select project which you have created in previous step

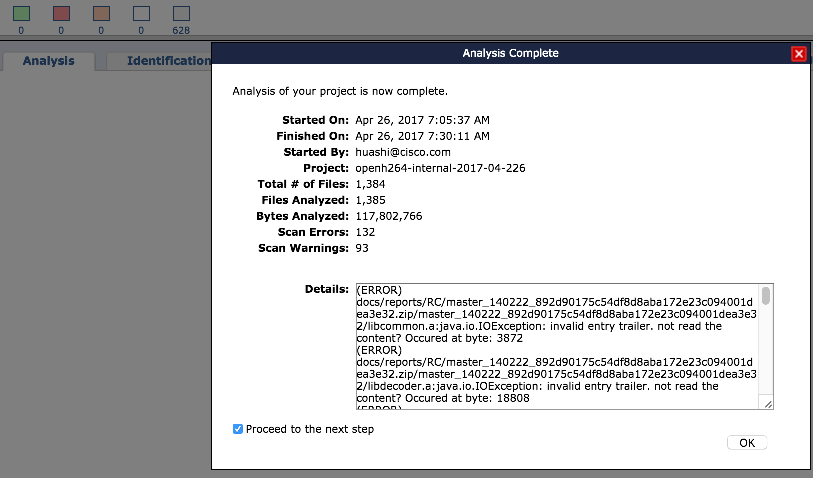


**Step 2,** Clice **Analysis** and click **Analyze Now** to scan code



**Step 3,** wait for scan result



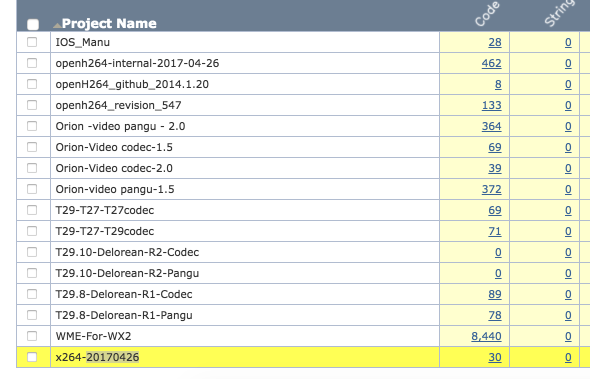


# **Check Analysis result**

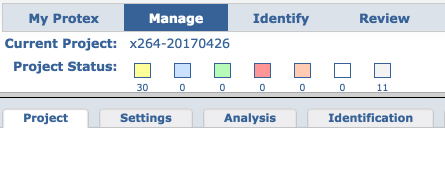
**4.1 basic check**

**Take x264 project for example;**

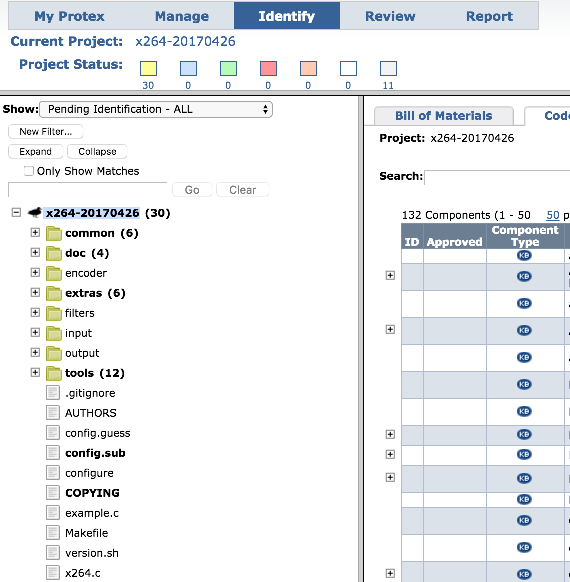
**Step 1**. Click **x264-20170416** as below



**Step 2** , click **project statu**s yellow square with 30 as show below



**Step 3**, Below shows which file may match third-party open source code



## **4.2 Analysis result for match code**

Take **code-coverage.sh** file for example;

Click **code-coverage.sh**;

And result shows that tow open source project matched with it

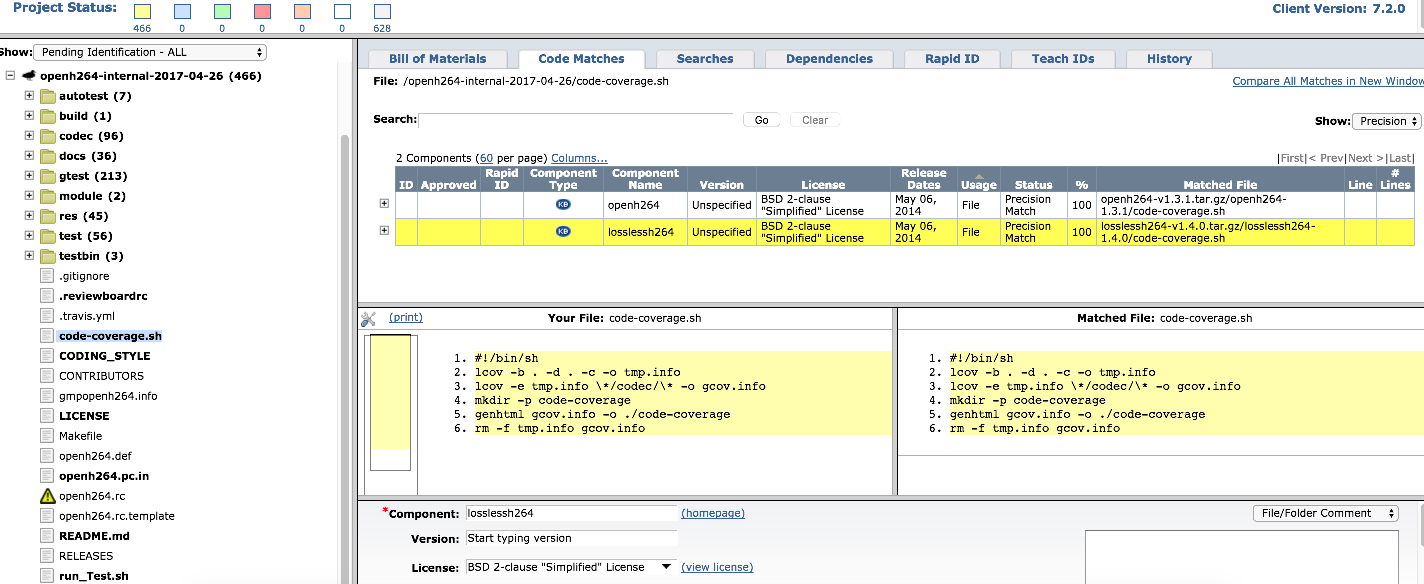
* openh264
* lossessh264

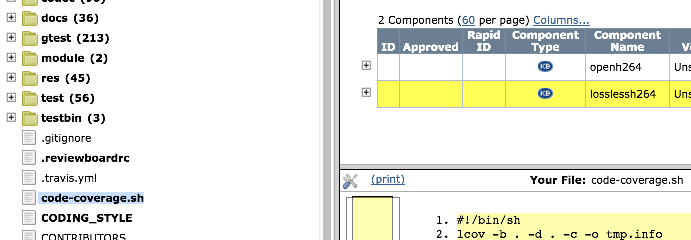
And click lossessh264,

Result shows that, they are same with each other which means 100% matched.

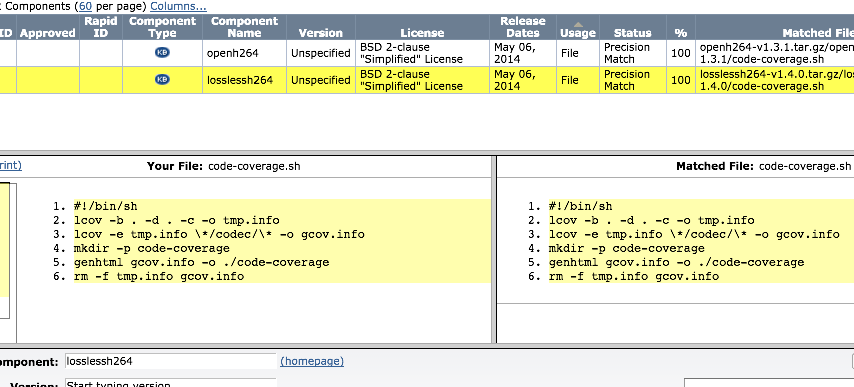
Double check lossessh264 project, go to its **home page**, which link to **github page**

And shows that it is forked from **cisco/openh264** project.

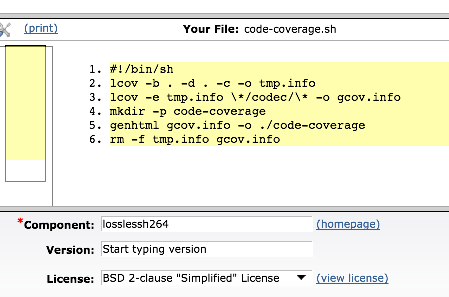




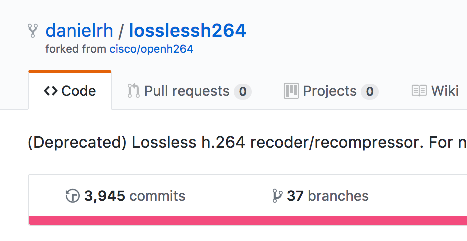
**100% matched**



**Home page info**



**home page links to github page, which shows it is forked from cisco/openh264**



# **IPCentral**

## **5.1 IPCentral basic**

* For project final code sign and open source scan/audit/report etc.
* For security audit etc.
* Login with CEC ID
* Project owner/module owner

## **5.2. WME in IPCentral**

**Wiki**

<https://wiki.cisco.com/display/CWMMF/IPCentral+for+WME>

**IPCentral**:

# Whiteny\_MediaSDK-SQBU

<http://ipcentral.cisco.com/ipcentral/jsp/ipcentral.jsp?component=ProjectView&entityId=59351615>

# WME\_Media\_Common

<http://ipcentral.cisco.com/ipcentral/jsp/ipcentral.jsp?component=ProjectView&entityId=60158994>