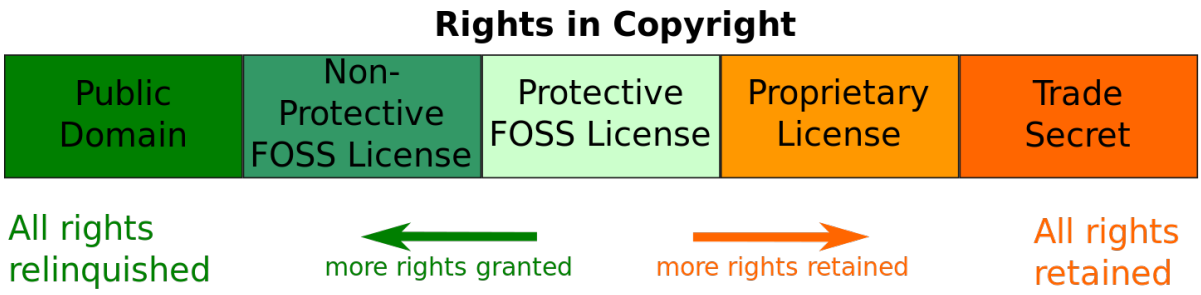
Open source scan

Table of Contents

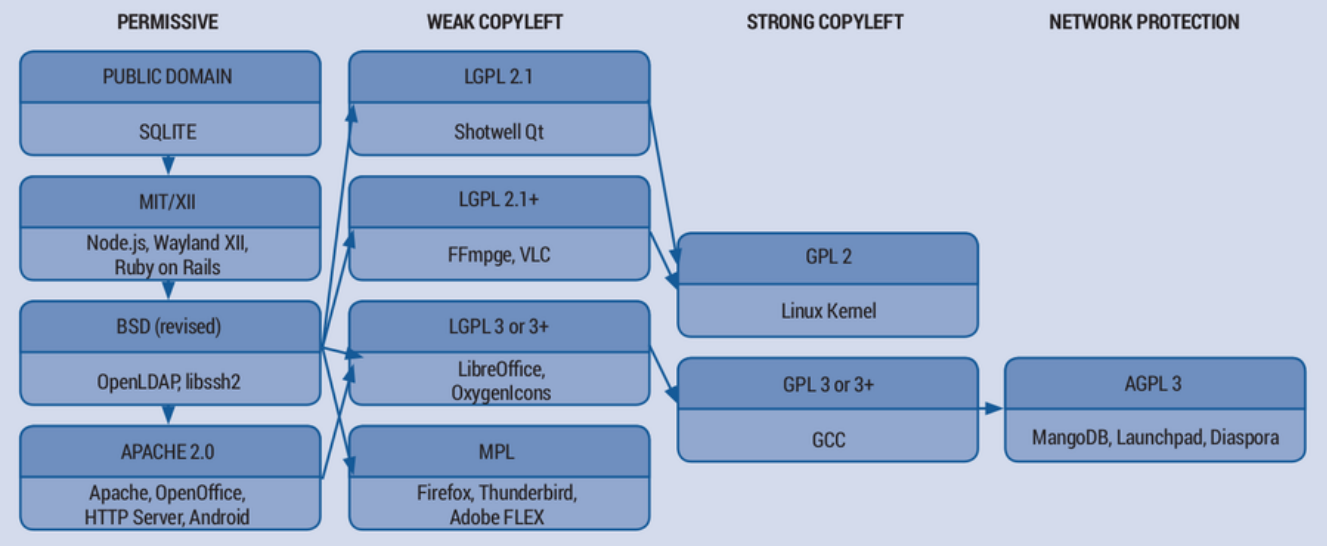
1. License

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

2. 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

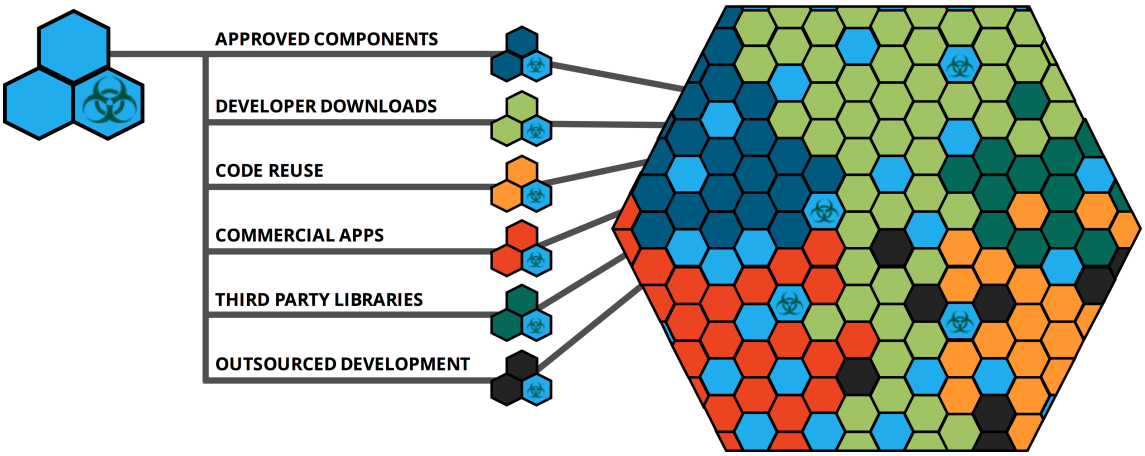
Product/solution:

Open Source Compliance & Management

Black Duck® Protex™ 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

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

online scan result:

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

local scan via client:

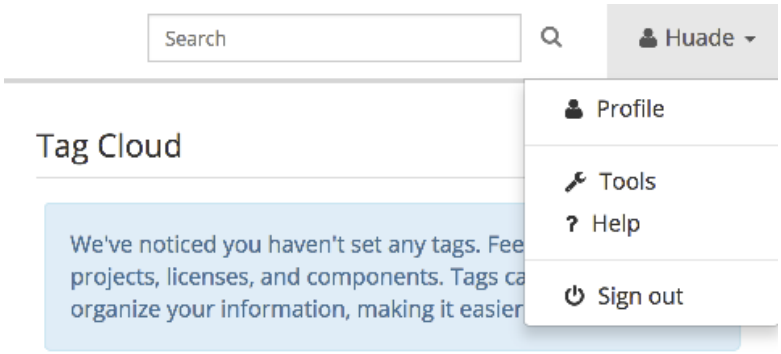
http://localhost:9000

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

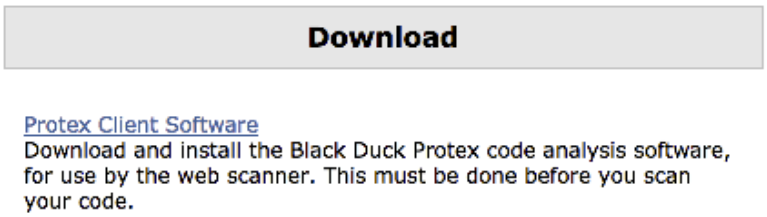
2.3 Download Blackduck

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



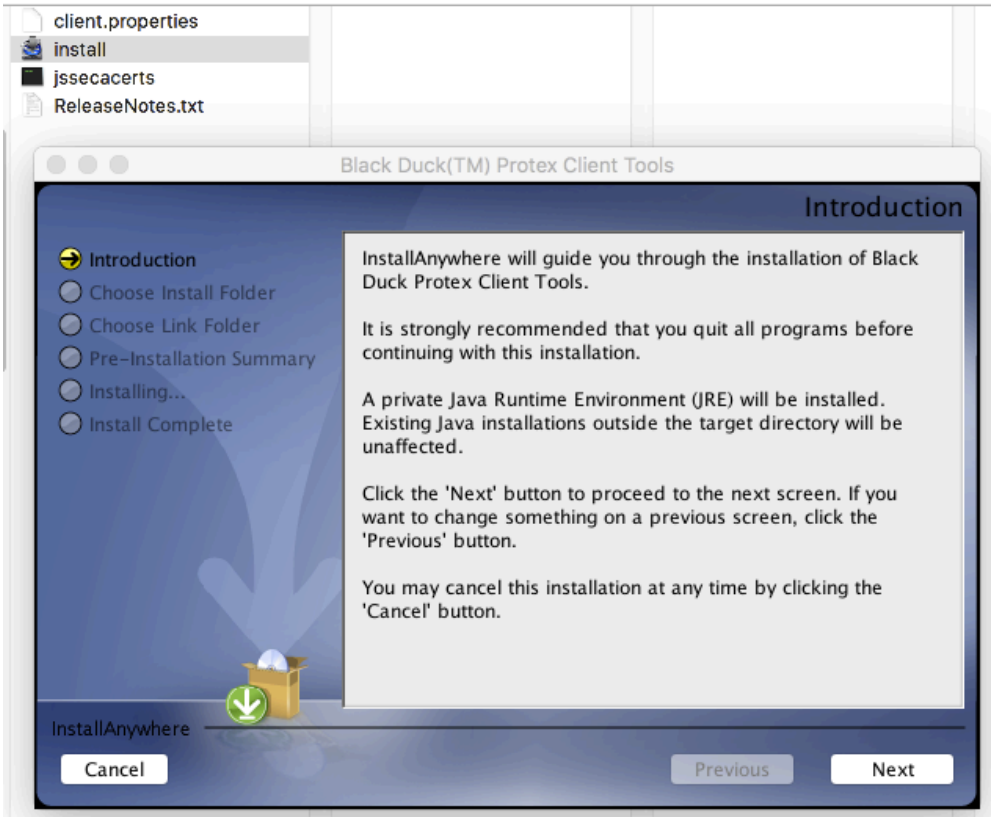
Step 3. Then click **Protex Client Software** as show below



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

2.4. install Blackduck

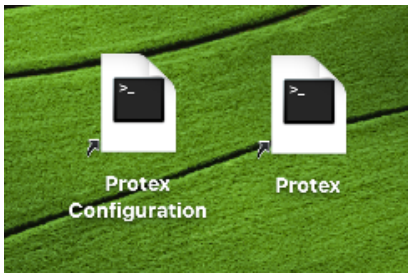
After download, click install file to install **protex client**.
Below shows the installation on mac



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



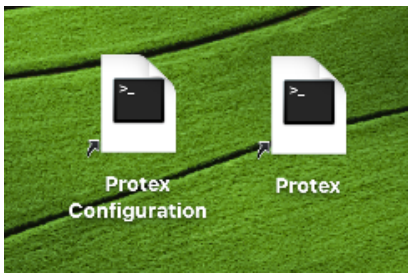
Step 1, click **Protex Configuration** for server URL setting
Will direct to below web page for URL setting
http://localhost:9000/client/setPrefs.jsp

Step 2, setting server URL for **Protex**
http://sjc-ipaudit-1.cisco.com is preferences setting

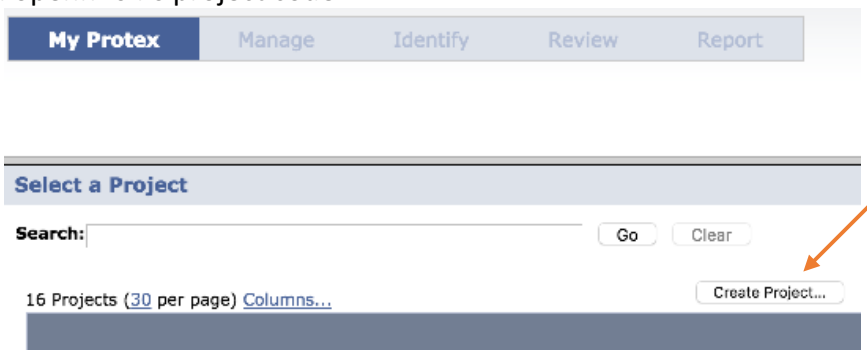
3. Scan code with Blackduck tool

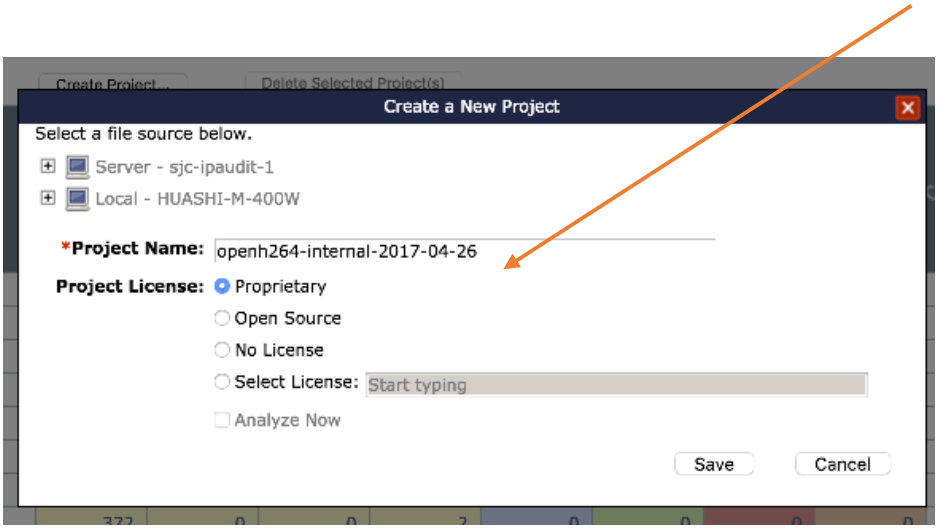
3.1 Create scan project

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

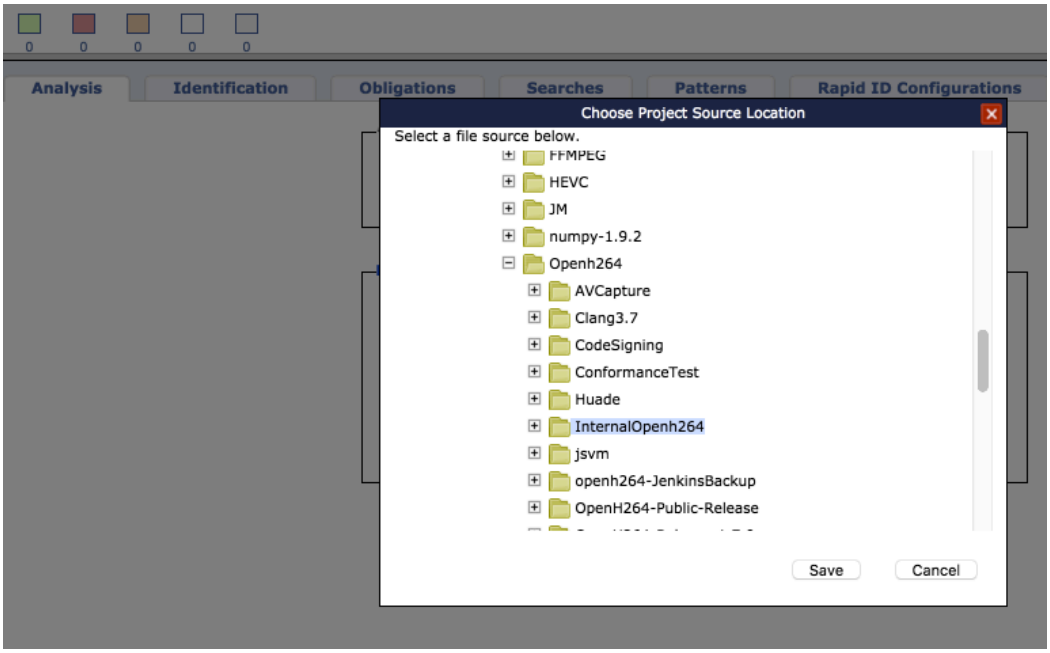


Step 2; Click Create Project to create one project for code scanning
Below shows create one openh264-internal-2017-04-26 project to scan latest internal openh264's project code



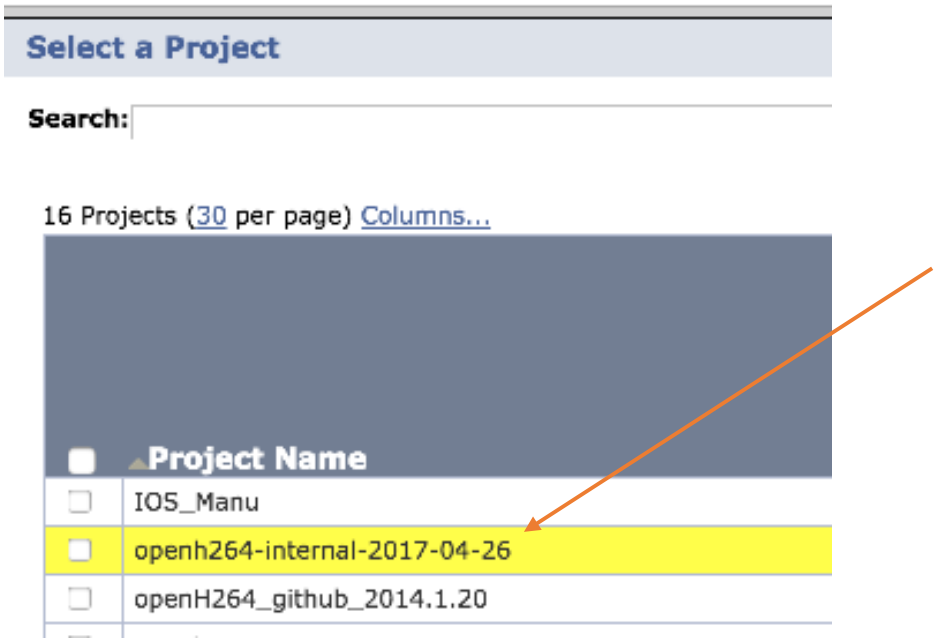


Step 3, Choose local code location and then click save

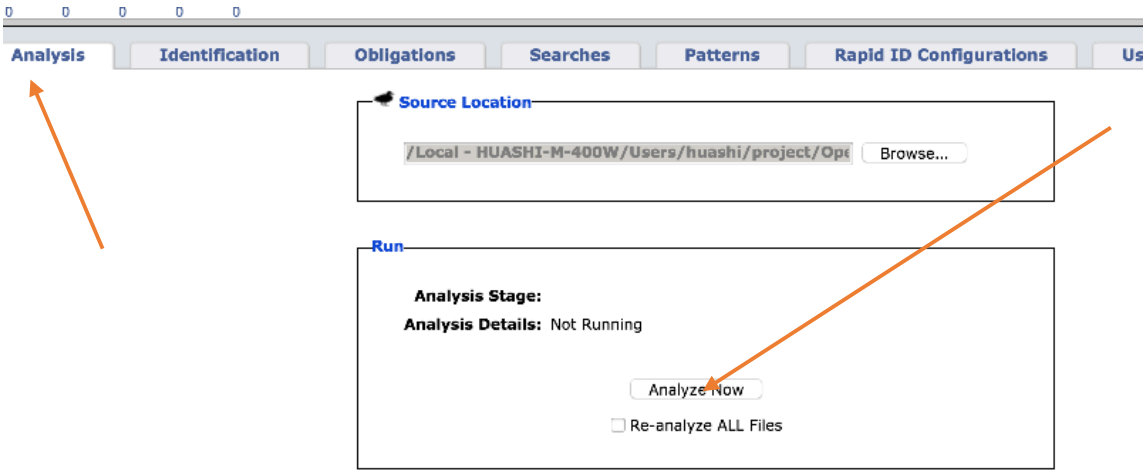


3.2. Analysis project code

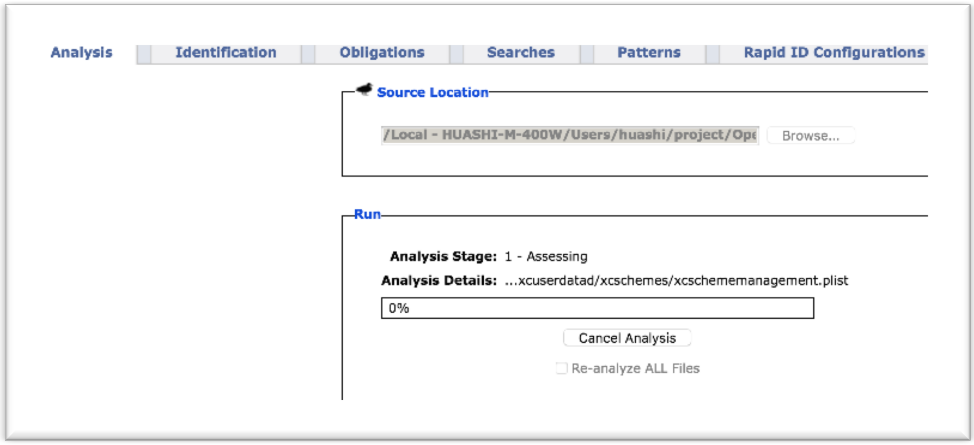
Step 1, Select project which you have created in previous step

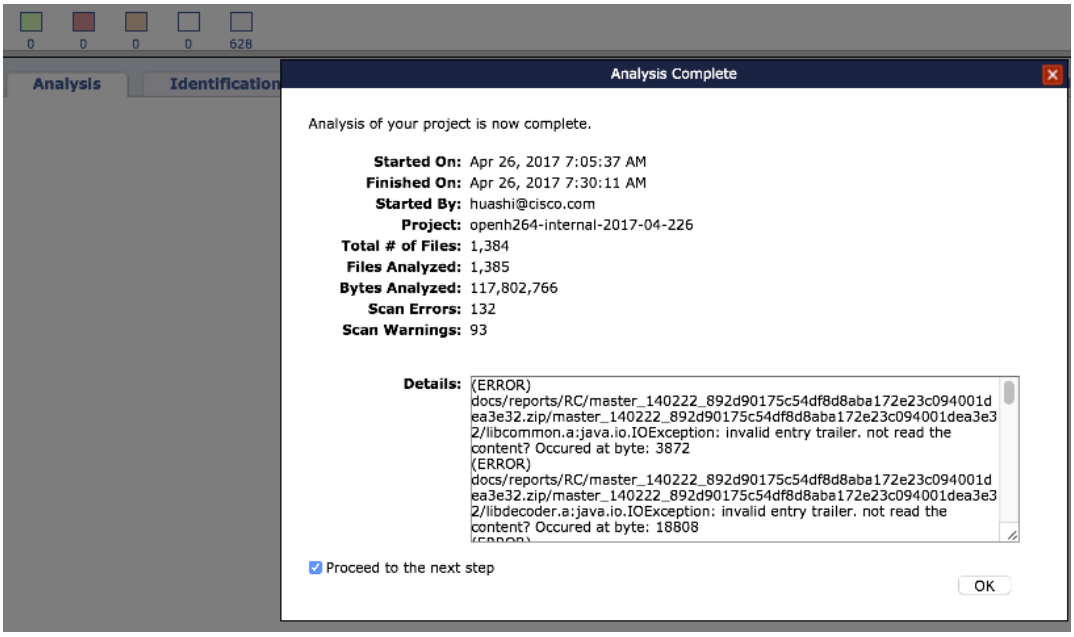


Step 2, Clice **Analysis** and click **Analyze Now** to scan code



Step 3, wait for scan result



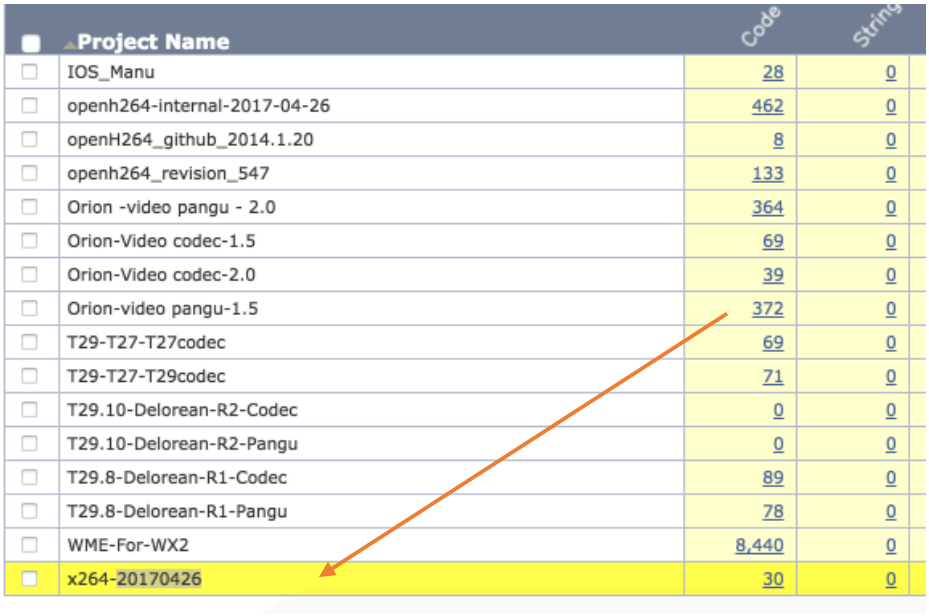


4. Check Analysis result

4.1 basic check

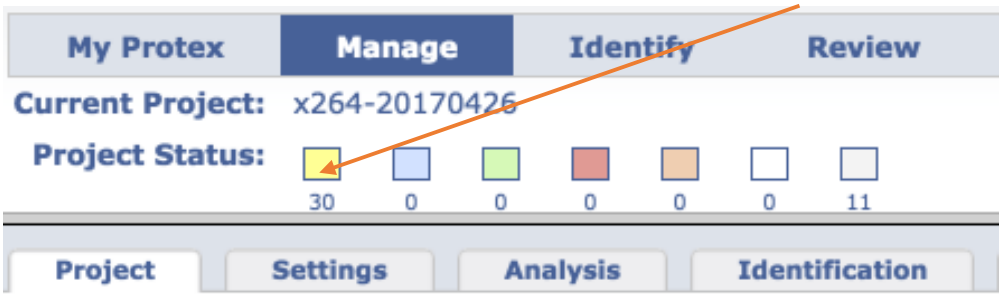
Take x264 project for example;

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

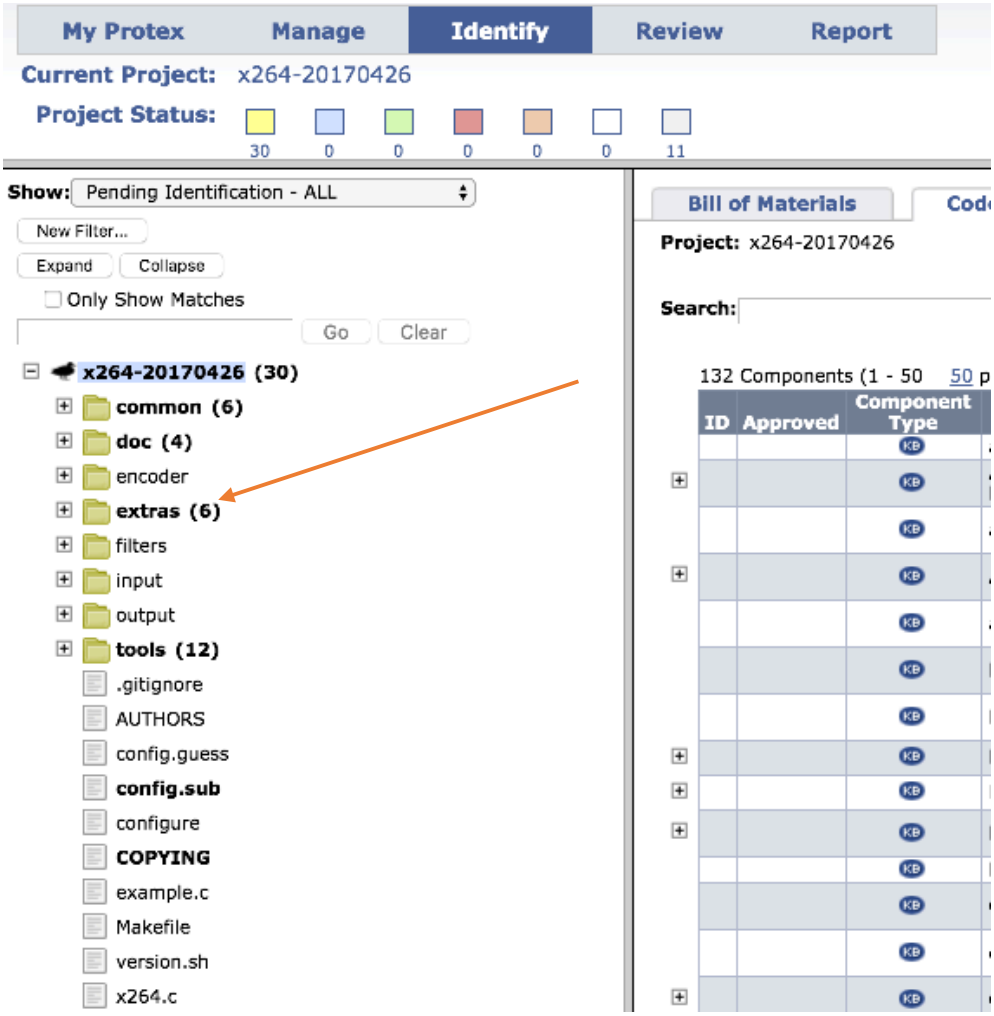


Project Name	Code	String
IOS_Manu	28	0
openh264-internal-2017-04-26	462	0
openH264_github_2014.1.20	8	0
openh264_revision_547	133	0
Orion -video pangu - 2.0	364	0
Orion-Video codec-1.5	69	0
Orion-Video codec-2.0	39	0
Orion-video pangu-1.5	372	0
T29-T27-T27codec	69	0
T29-T27-T29codec	71	0
T29.10-Delorean-R2-Codec	0	0
T29.10-Delorean-R2-Pangu	0	0
T29.8-Delorean-R1-Codec	89	0
T29.8-Delorean-R1-Pangu	78	0
WME-For-WX2	8,440	0
x264-20170426	30	0

Step 2 , click **project status** 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

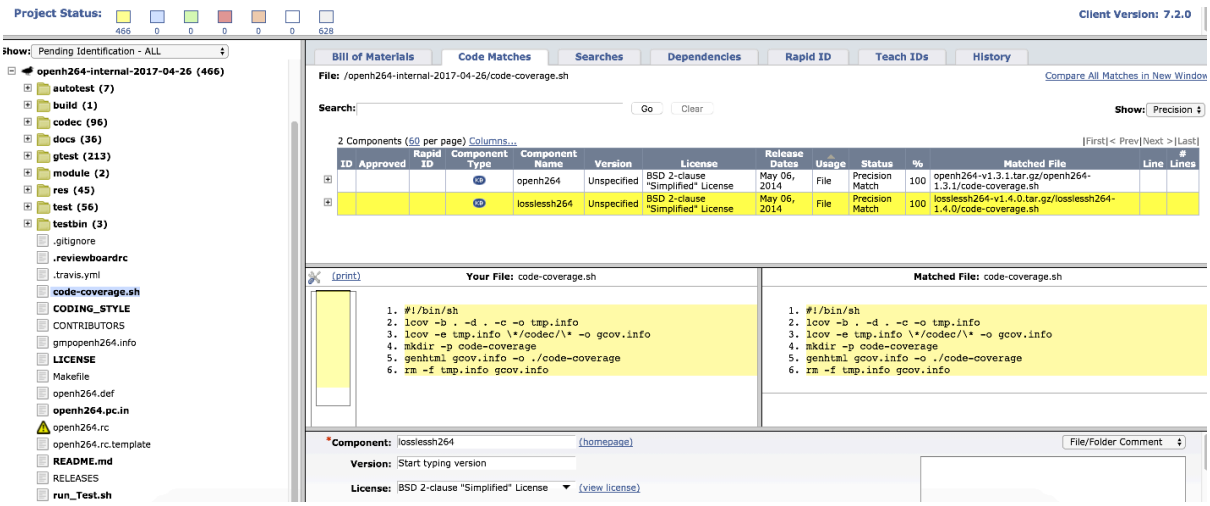
Take **code-coverage.sh** file for example;

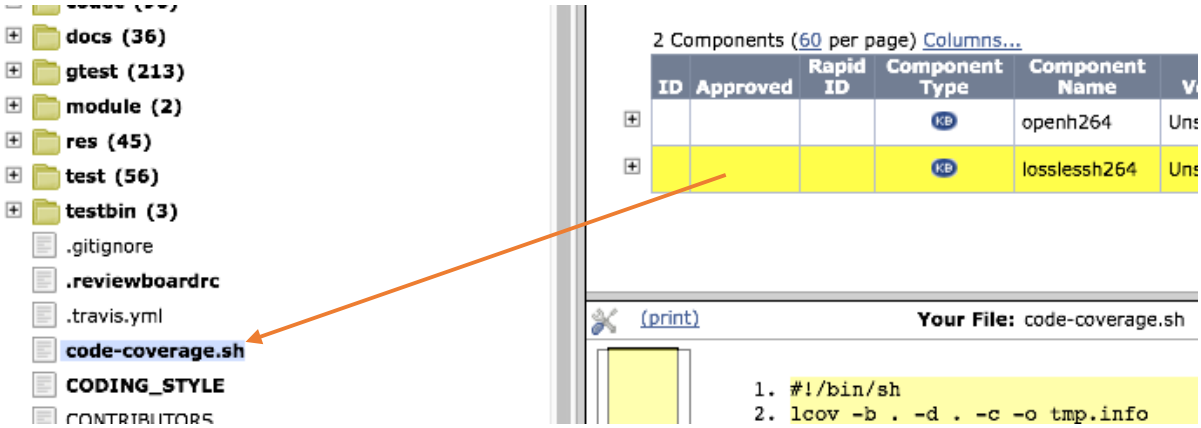
Click **code-coverage.sh**;
And result shows that tow open source project matched with it

- openh264
- lossessh264

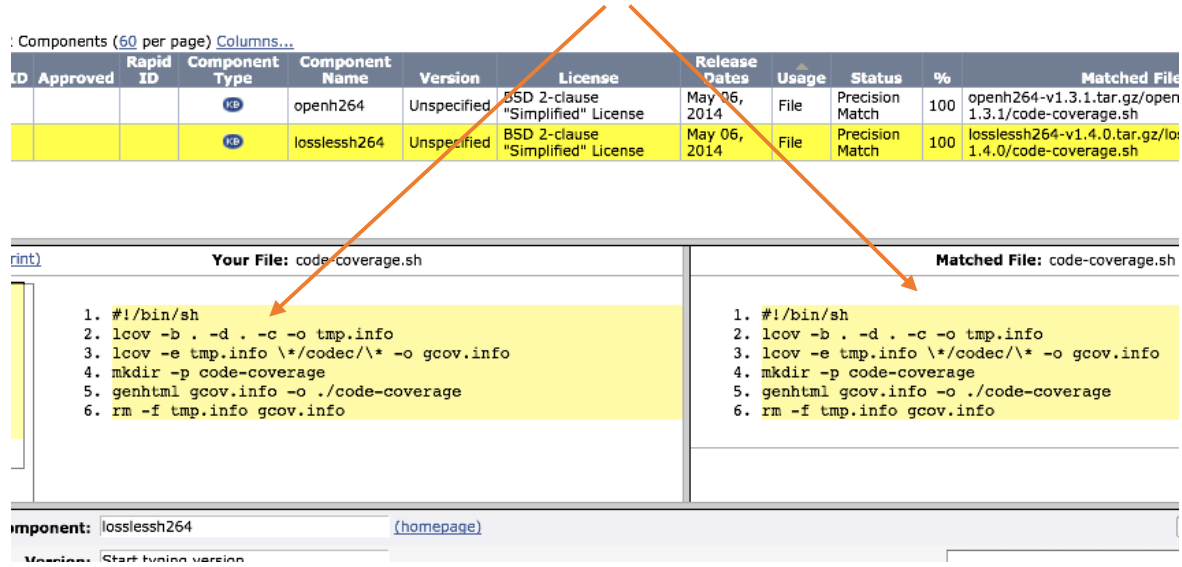
And click lossessh264,
Result shows that, they are same with each other which means 100% matched.

Double check lossessh264 project, go to its **home page**, which link to **github page**
And shows that it is forked from **cisco/openh264** project.

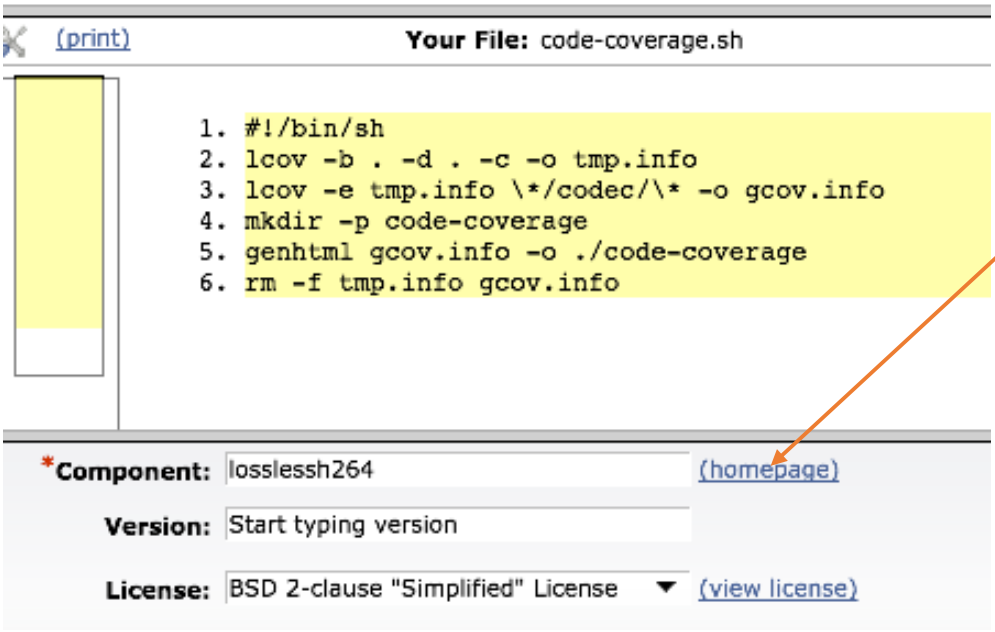



docs (36)
gtest (213)
module (2)
res (45)
test (56)
testbin (3)
.gitignore
.reviewboardrc
.travis.yml
code-coverage.sh
CODING_STYLE
2 Components (60 per page) Columns...
ID
Approved
Rapid ID
Component Type
Component Name
openh264
losslessh264
(print)
Your File: code-coverage.sh
1. #!/bin/sh
2. lcov -b . -d . -c -o tmp.info

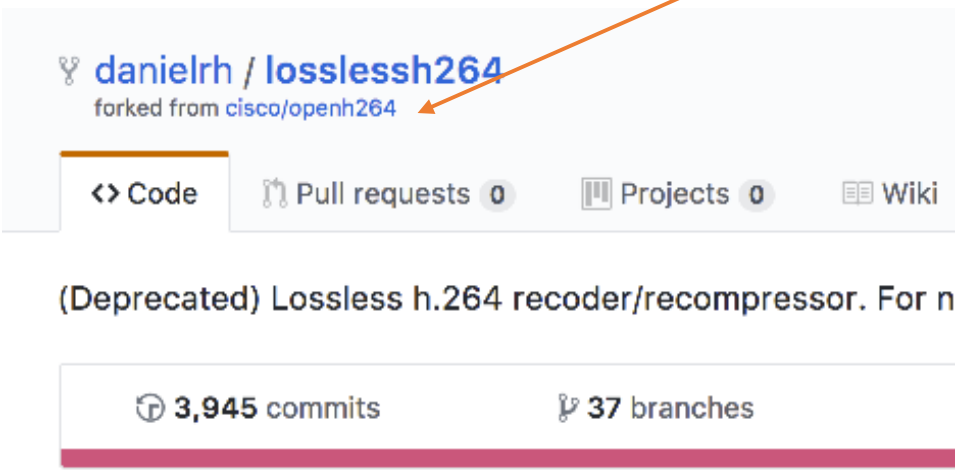
100% matched


Components (60 per page) Columns...
Approved
Rapid ID
Component Type
Component Name
Version
License
Release Dates
Usage
Status
%
Matched File
openh264
Unspecified
BSD 2-clause "Simplified" License
May 06, 2014
File
Precision Match
100
losslessh264
Unspecified
BSD 2-clause "Simplified" License
May 06, 2014
File
Precision Match
100
Your File: code-coverage.sh
Matched File: code-coverage.sh
1. #!/bin/sh
2. lcov -b . -d . -c -o tmp.info
3. lcov -e tmp.info */codec/* -o gcov.info
4. mkdir -p code-coverage
5. genhtml gcov.info -o ./code-coverage
6. rm -f tmp.info gcov.info
losslessh264
(homepage)

Home page info



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



5. 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