SET UP FROM SCRATCH

SET UP FROM SCRATCH

- Requirements
  - Hardware
  - Software
  - Download Link
- Install
  - Target Software Install
    - Adobe Acrobat Reader
    - Foxit PDF Reader
  - TypeOracle Set Up
    - Python
    - 7-Zip
    - IDA pro
    - Windbg
    - Pin
    - DynamoRIO
    - Favocado related
    - TypeOracle Tool
- what the artifacts do
- how to reproduce

Requirements

Hardware

- 2-core CPU and 4G memory at least
- storage: 50G at least

Software

- OS: Windows 8.1
- Python 3.8.9 and Python2 .7.17 (pywinauto, psutil need to be installed)
- Adobe Acrobat Reader (32bit, English version: 19.021.20048, 20.013.20074, 21.011.20039, installed in the default directory)
- Foxit PDF Reader (32bit, English version: 10.1.1,11.2.1, installed in the default directory.)
- IDA pro v7.0
- Windbg
- Pin v3.17
- DynamoRIO
- 7-zip

Download Link

InstallPackages: https://drive.google.com/file/d/1hls-L8OuoYp2cvwnmshWypMNbcopEXZ8/view

TypeOracle: https://drive.google.com/file/d/1S4YwbkNX8_SxhDVppZL6h3sRc4ZPYzle/view

Install

Target Software Install

In our experiment, we test our tool on two PDF Readers, Adobe Acrobat Reader and Foxit PDF Reader.

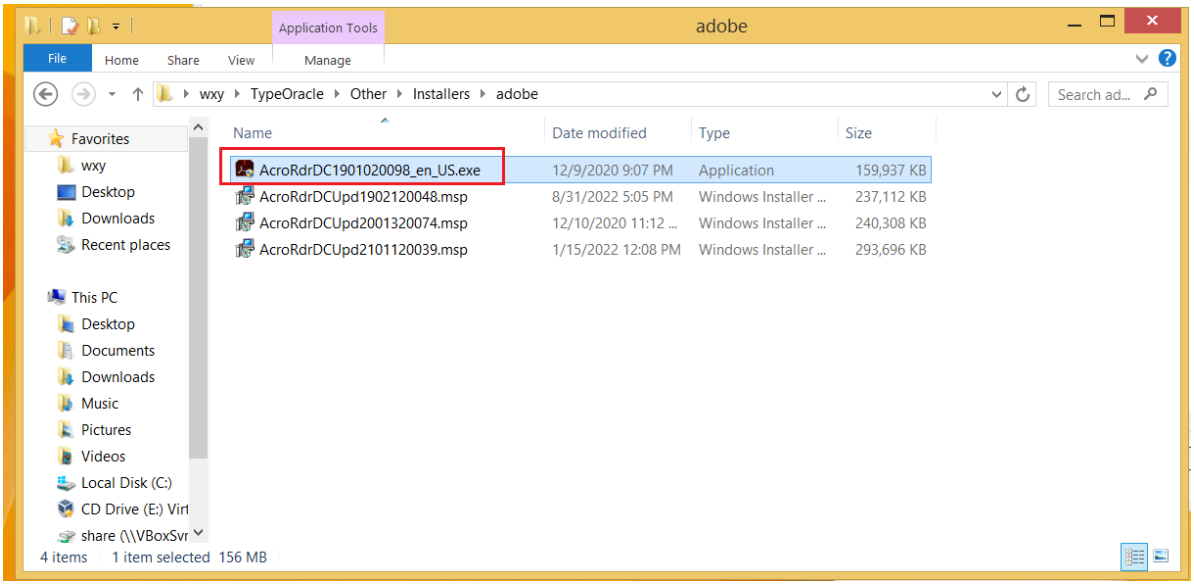
Adobe Acrobat Reader

For Adobe Acrobat Reader, you can download it from https://helpx.adobe.com/acrobat/release-note/release-notes-acrobat-reader.html. You can also find the install packages in `InstallPackages\TargeSoftware`.

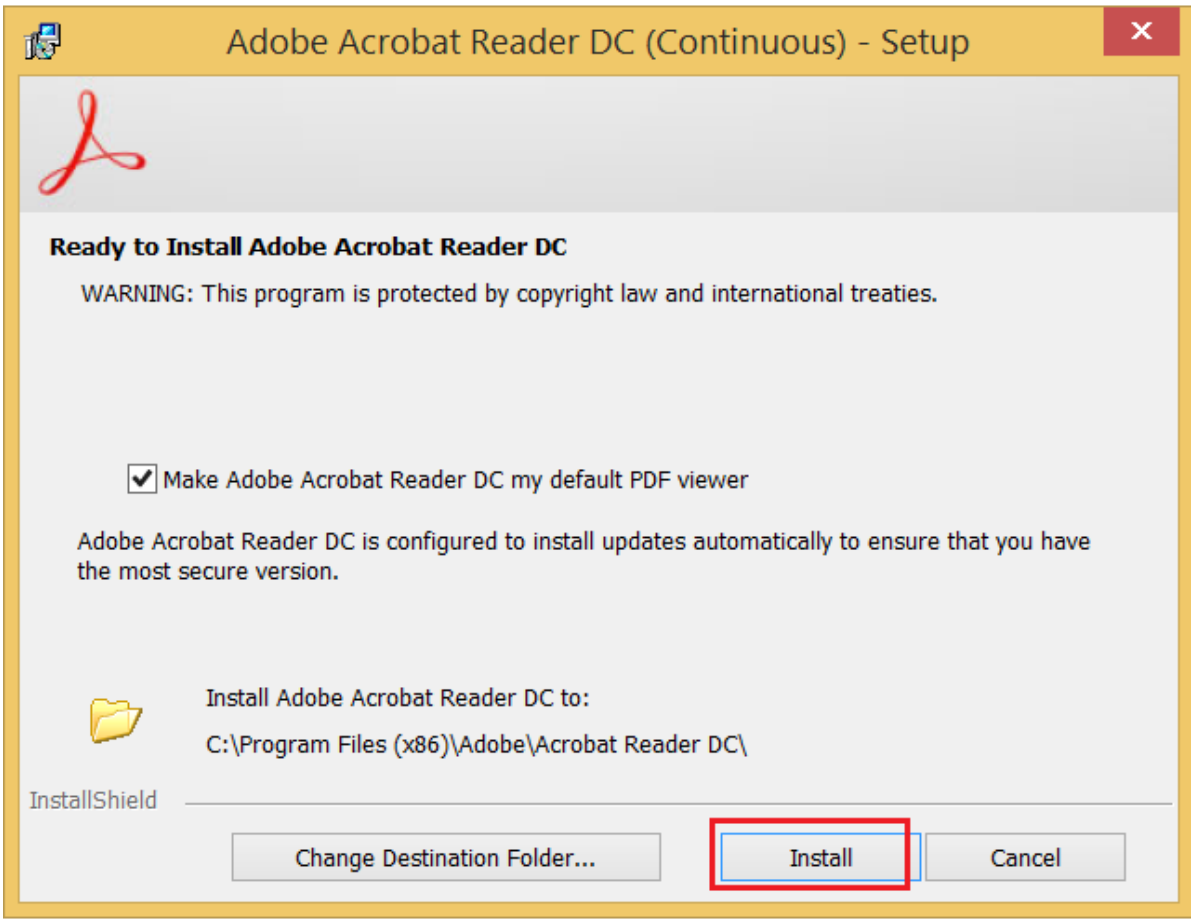
Acrobat and Acrobat Reader Continuous Track release notes

Date	Release Notes	Release Type*	Focus
Nov 17, 2022	DC Nov 2022 (22.003.2028x)	Optional Update	**Latest Release:** This patch fixes specific functionality issues.
Oct 22, 2022	DC Oct 2022 (22.003.20263)	Optional Update	**[Win Only]** This patch fixes specific functionality issues.
Oct 11, 2022	DC Oct 2022 (22.003.20258)	Continuous	This update provides new features, feature enhancements, and bug fixes.
Sep 09, 2022	DC Sep 2022 (22.002.20212)	Optional Update	This patch fixes specific functionality issues.
Aug 09, 2022	DC Aug 2022 (22.002.20191)	Continuous	This update provides security mitigations and bug fixes.
Jul 12, 2022	DC Jul 2022 (22.001.20169)	Continuous	This update provides security mitigations and bug fixes.
Jun 14, 2022	DC Jun 2022 (22.001.20142)	Continuous	This update provides new features, feature enhancements, and bug fixes.

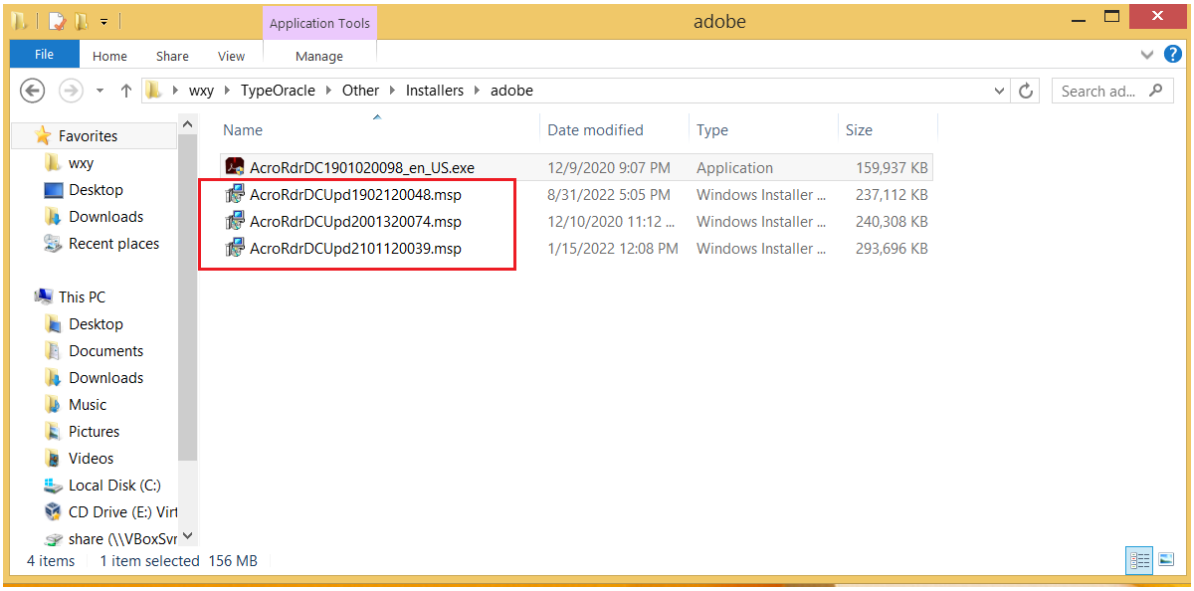
open this executable file to install the basic version of Adobe Reader



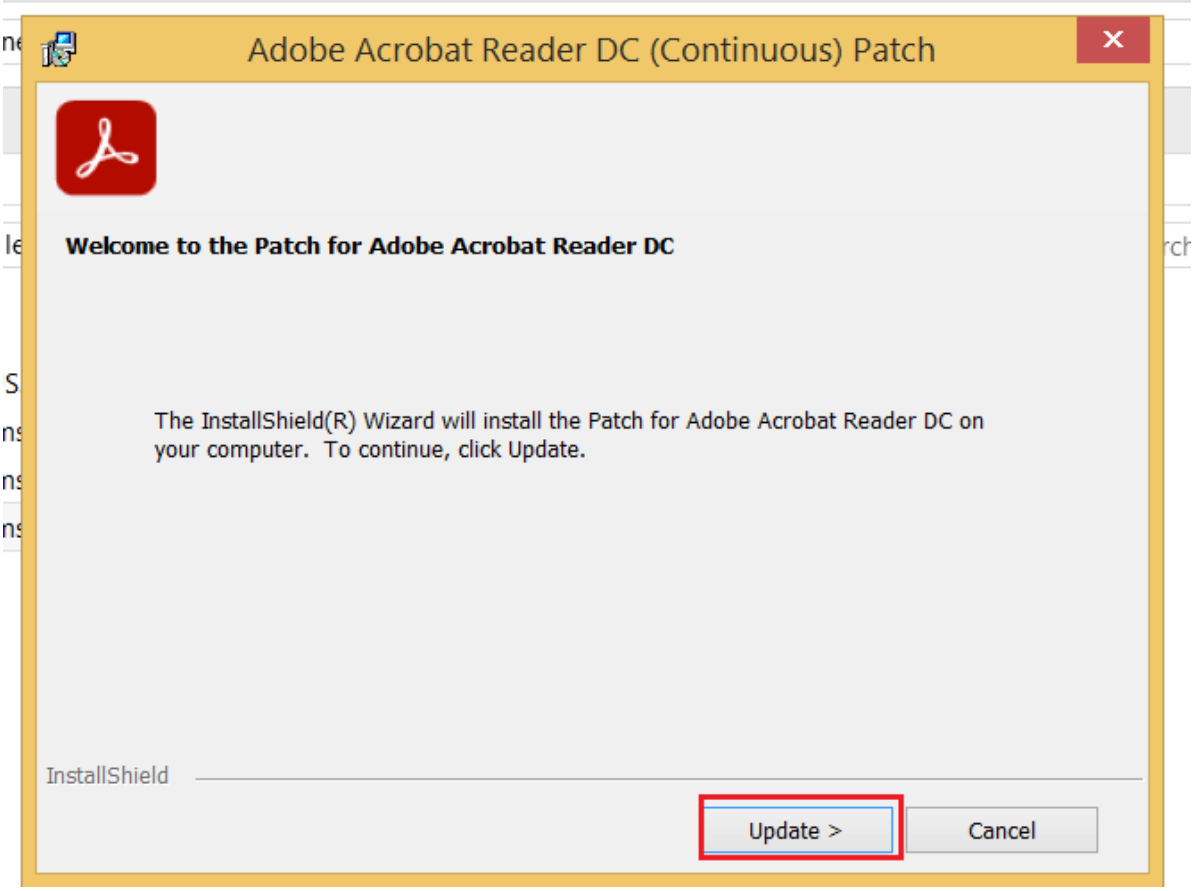
click the `install` button to start



choose the version you want to update to update the basic version to wanted version (we use 2021.011.20039 as an example)



click the `update` button to start



5. when the first time you open the Adobe Reader, you need to click the `Accept` button

Foxit PDF Reader

For Foxit PDF Reader, you can download it from https://www.foxit.com/pdf-reader/version-history.html. You can also find the install packages in `InstallPackages\TargeSoftware`.

Foxit PDF Reader Version History

Version 12.1.0.15250

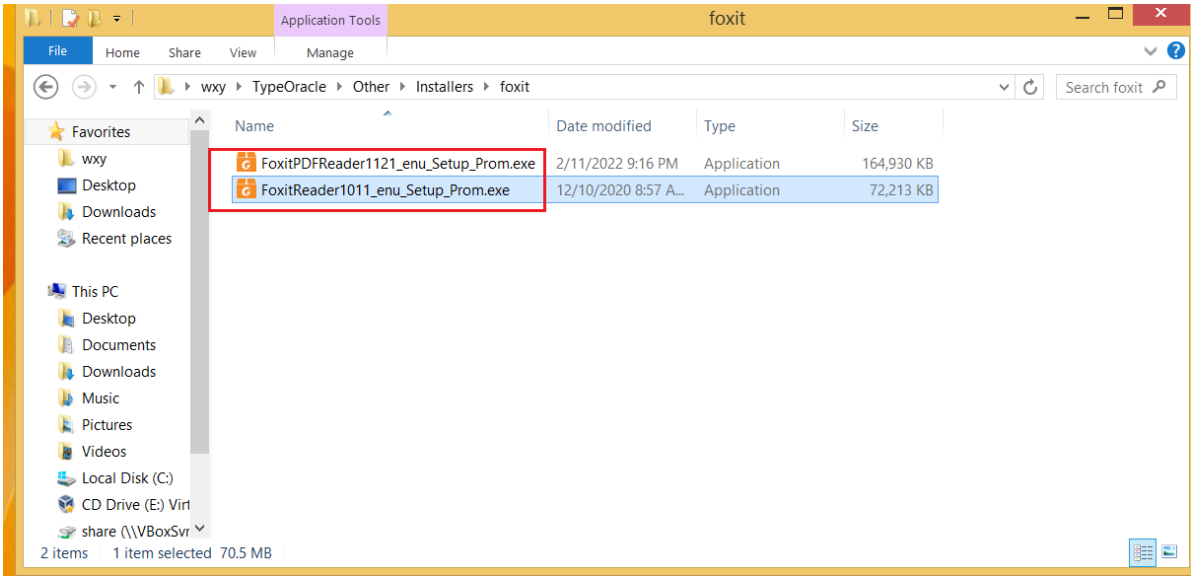
Release Date: December 13, 2022

Download >>

New Features and Improvements in Foxit PDF Reader 12.1.0.15250

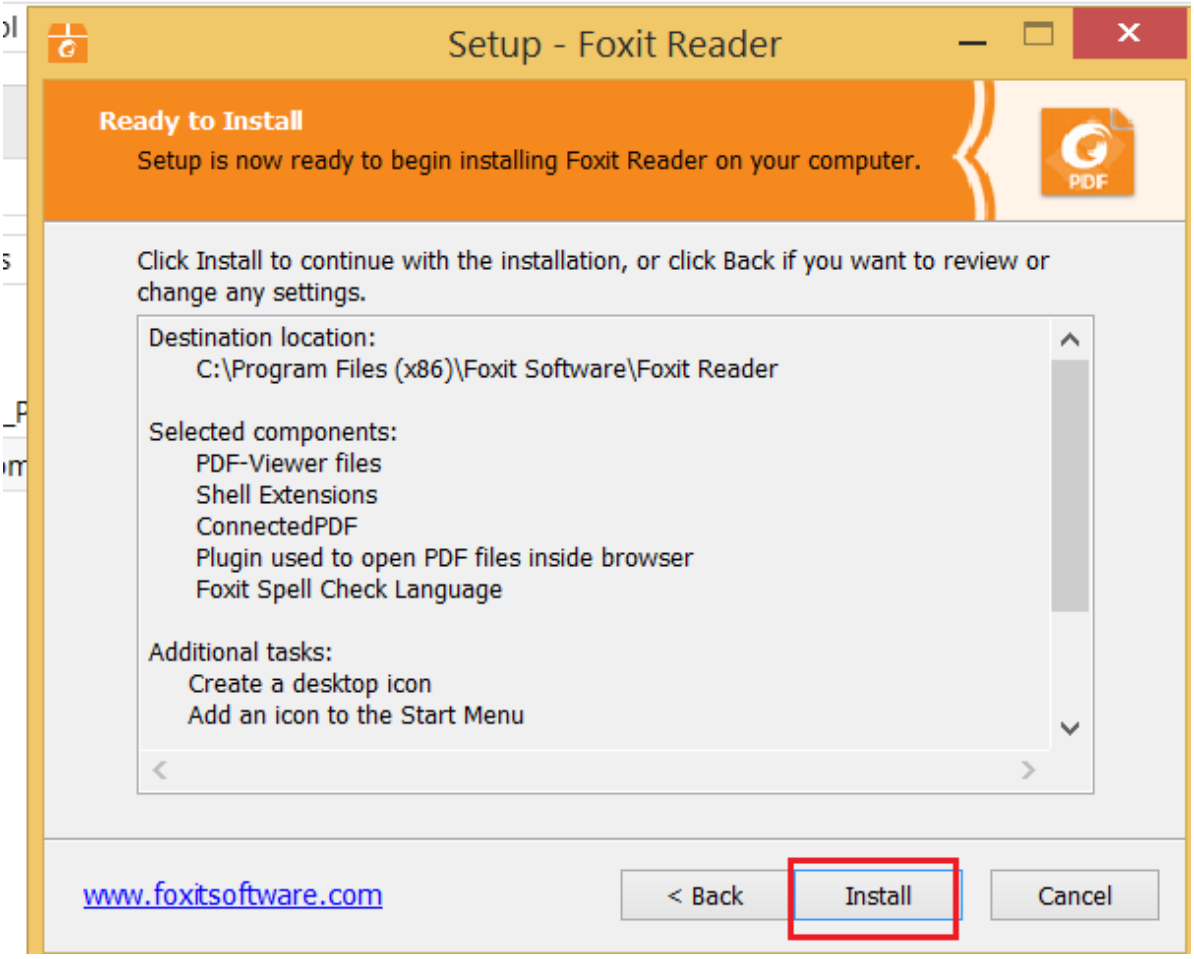
- Improved compatibility with Windows 11 UI style
  - Show the Snap layouts when you hover the mouse over the application window's maximize button.
  - Round the window corners of the application's main window, dialog boxes, and drop-down menus.

choose the version you want to install (we use 10.1.1 as an example)



just use the default settings to install (click the `next` button)

after several times of clicking `next` button, you will see this page, and click `install` button to start



TypeOracle Set Up

Python

Since most parts of our tool is implemented by python, so if the python is installed, our tools can run normally.

Python 3 can be downloaded from https://www.python.org/downloads/release/python-389/.

Python 2 can be downloaded from https://www.python.org/downloads/release/python-2717/.

In order to run our tool, some python packages need to be installed, they are `psutil` and `pywinauto`.

You can install these two packages by the following commands

```
pip install pywinauto
pip install psutil
```

7-Zip

Our tool utilize 7-zip to zip and unzip the coverage information during coverage recording. You can download it from https://www.7-zip.org/. You can also find it in the provided `InstallPackages\TypeOracleNeed`.

7-Zip

7-Zip is a file archiver with a high compression ratio.

Download 7-Zip 22.01 (2022-07-15) for Windows:

Link	Type	Windows	Size
Download	.exe	64-bit x64	1.5 MB
Download	.exe	32-bit x86	1.2 MB
Download	.exe	64-bit ARM64	1.5 MB

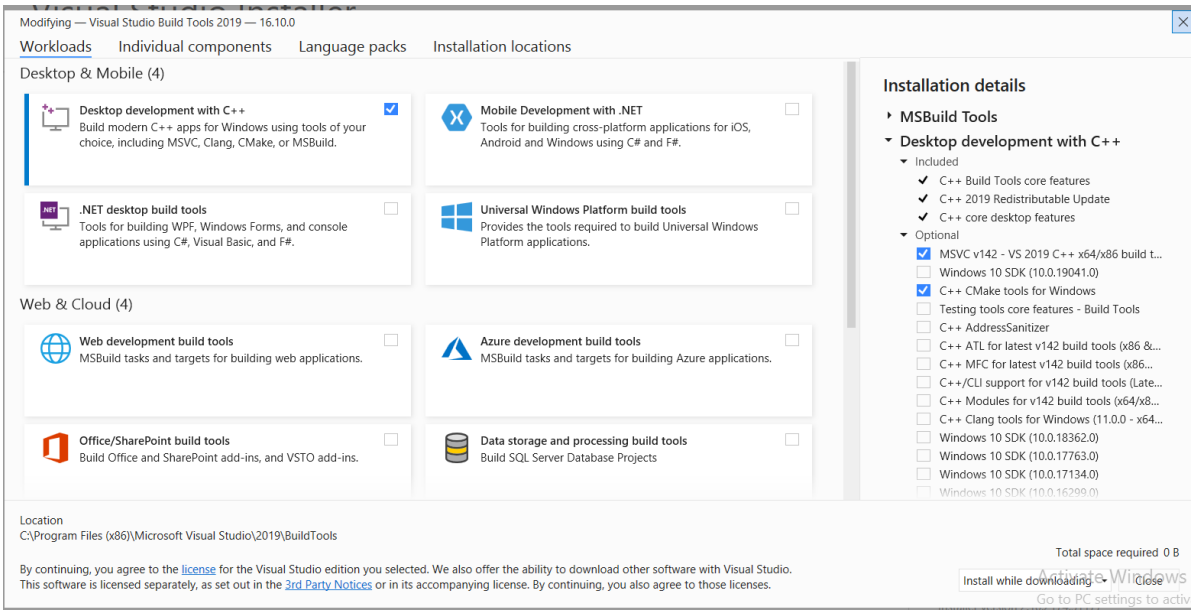
IDA pro

IDA pro is used in the Type Inference component of our tool, we provide a copy of IDA pro in the `InstallPackages\TypeOracleNeed`.

Windbg

Windbg is a very useful tool developed by Microsoft to debug programs. It is integrated in Visual Studio, so we have to install windbg by Visual Studio Installer.

The following is the setting to install windbg.



Pin

Besides python, our tool use pin.exe to instrument the PDF Readers, you can download pin from https://www.intel.com/content/www/us/en/developer/articles/tool/pin-a-binary-instrumentation-tool-downloads.html. You can also find it in the provided `InstallPackages`, you can unzip `InstallPackages\TypeOracleNeed\pin-3.17.7z` and place the pin-3.17 folder to `C:\Users\wxy\Desktop\pin-3.17` for our tool.

> Downloads
>
> Download Pin kits here. Before using Pin, please read the license.
>
> Windows*
>
> IA32 and intel64 (x86 32 bit and 64 bit)

Version	Date	Kit	Documentation		
Pin 3.25	October 20, 2022	98650	Manual	PinCRT	Release Notes
Pin 3.24	July 18, 2022	98612	Manual	PinCRT	Release Notes
Pin 3.23	May 12, 2022	98579	Manual	PinCRT	Release Notes
Pin 3.22	February 28, 2022	98547	Manual	PinCRT	Release Notes
Pin 3.21	October 28, 2021	98484	Manual	PinCRT	Release Notes
Pin 3.20	July 12, 2021	98437	Manual	PinCRT	Release Notes

> View all

DynamoRIO

You also need to install DynamoRIO, you can download it from https://dynamorio.org/page_releases.html. Our version is https://github.com/DynamoRIO/dynamorio/releases/download/release_8.0.0-1/DynamoRIO-Windows-8.0.0-1.zip. You can also find it in the provided `InstallPackages`, you can unzip `InstallPackages\TypeOracleNeed\DynamoRIO.7z` and place the DynamoRIO folder to `C:\Users\wxy\Desktop\DynamoRIO` for our tool.

Releases

For the very latest changes since the last official release, you can download **Weekly Builds**.

The 9.0.1 release:

- DynamoRIO-Windows-9.0.1.zip
- DynamoRIO-Linux-9.0.1.tar.gz
- DynamoRIO-ARM-Linux-EABIHF-9.0.1.tar.gz
- DynamoRIO-ARM-Android-EABI-9.0.1.tar.gz
- DynamoRIO-AArch64-Linux-9.0.1.tar.gz

The prior 8.0.0 release:

- DynamoRIO-Windows-8.0.0-1.zip
- DynamoRIO-Linux-8.0.0-1.tar.gz
- DynamoRIO-ARM-Linux-EABIHF-8.0.0-1.tar.gz
- DynamoRIO-ARM-Android-EABI-8.0.0-1.tar.gz
- DynamoRIO-AArch64-Linux-8.0.0-1.tar.gz

Favocado related

Favocado is a state-of-the-art fuzzer that consider binding calls during fuzzing. Our tool can be complementary with it by providing more complete and accurate parameter type information.

In order to use Favocado, you need to install ruby and nodejs, we have also provided these installers in `InstallPackages\TypeOracleNeed`

Favocado

Prerequisites

- Node
- [origami] (https://github.com/gdelugre/origami)

TypeOracle Tool

You can find our tool in the provided `TypeOracle` zip file, you should unzip it and place TypeOracle folder to `C:\Users\wxy\TypeOracle`.

what the artifacts do

Our artifacts include three components, type inference, fuzzer and coverage collecting.

For the type inference component, our tool uses differential analysis to reason about the type information of the binding calls in PDF Readers.

For the fuzzer component, our tool uses the type information to guide the generation of test PDFs.

For coverage collecting component, our tool uses DynamoRIO to collect the coverage information when running test PDFs.

how to reproduce

For the reproduction of RQ1 and RQ2, please refer to the type inference component of our tool. which are `TypeOracle\Tools\TypeInfer\adobe\README.pdf` for type inference in Adobe Reader and `TypeOracle\Tools\TypeInfer\foxit\README.pdf` for type inference in Foxit Reader. After getting the type information, you can compare it with the ground truth, which is located in `data/ground_truth` folder, please refer to `TypeOracle\Evaluation\RQ1_TypeAccuracy\README.pdf`. As for other type inferring methods, please refer to `TypeOracle\Other\TypeInfer`.

For the reproduction of RQ3, please refer to the fuzzer component and coverage collecting component of our tool. First, you need to run the fuzzer for 48 hours to generate some PDF files, please refer to `TypeOracle\Tools\Fuzzer\README.pdf` to use the fuzzer of TypeOracle. As for other fuzzers, please refer to `TypeOracle\Other\Fuzzer`. After executing the fuzzer for 48 hours, you need to use the coverage collecting component to collect the coverage information. For the coverage collecting, please refer to `TypeOracle\Tools\Coverage\README.pdf`.

For the reproduction of RQ4, please refer to the fuzzer component of our tool. The PDFs which can cause PDF Readers to crash will be stored in `save/crash` folder, please refer to `TypeOracle\Evaluation\RQ4_FuzzingCampaign\README.pdf` for manually check.

For some tips that may be helpful for the reproduction, please refer to `TypeOracle\Other\Tips.pdf`