Crypto Metrics Tool v0.3.5 User Manual

Katarzyna Mazur

July 14, 2014

CMTOOL

Contents

1	$\mathbf{C}\mathbf{M}$	Tool's	Overview	2
	1.1	Interfa	ace Guide	2
2	$\mathbf{C}\mathbf{M}$	Tool's	Installation Guide	9
	2.1	Install	ation Guide for GNU/Linux-like Operating Systems	9
		2.1.1	CMTool Console Version - Installation	9
		2.1.2	CMTool GUI Version - Installation	16
	2.2	Install	ation Guide for Microsoft Windows-like Operating Systems	21
		2.2.1	CMTool Console Version - Installation	21
		2.2.2	CMTool GUI Version - Installation	24
3	$\mathbf{C}\mathbf{M}$	Tool's	Screenshoots	26

CMTool's Overview

1.1 Interface Guide

Main window of the *CMTool* in GUI mode looks like below (see Fig. 1.1):

	Crypto Metrics Tool v0.3.5		(v) (c)
e <u>F</u> audnade iuro	Πεφ		
Benchmarking Para	meters Jalidation Parameters		
	Benchmarking input parameters		
Benchmark:	Encryption/Signing	✓ Tests:	0 0
	All	A	
Algorithms:	MD4	Iterations:	0 0
	MD5	× ×	
Parallel benchmarks:		Input's size [bytes]:	0 0
Number of parallel		(-)j-	
benchmarks:			1 🗘
		Benchmark	Cancel
	0%		
		(CMTO

Figure 1.1: *CMTool's* main window

CMTool in GUI mode is written with the use of the open source version of Qt library - that's why the whole interface of the application should look almost exactly the same no matter if one uses it on Microsoft Windows or GNU/Linux. At the top of the main window one can see a menu with some options described in detail below:

1. Menu File:

🌜 Clean stats	Ctrl+C
😗 Save stats as XML	Shift+X
Save stats as HTML	Shift+H
Export as QoP-ML security metric	Shift+Q
🔀 Exit	Ctrl+Q

Figure 1.2: Menu File has 5 items

- (a) Item **Clean stats** cleans information about calculated statistical primitives presented in a table located at the bottom of the main window
- (b) Item Save stats as XML saves obtained results into the *.xml file
- (c) Item **Save stats as HTML** saves obtained results into *.*html* files, makes simple documentation in html format
- (d) Item **Export as QoP-ML security metric** cleans information about calculated statistical primitives presented in a table located at the bottom of the main window
- (e) Item **Exit** saves obtained results into the *.qop file, in format which can be understood by the AQoPA
- 2. Menu **Language** lets user to change the language of the interface (not implemented yet)
- 3. Menu **Info** lets user get some information about the hardware and software of her/his machine on which *CMTool* was run (see Fig. 1.3). Using keyboard shortcut, CTRL+I, one is able to see information about the software and hardware of the machine on a new tabbed window which immediately appears (see Fig. 1.4 and 1.5).

Figure 1.3: With $Get\ machine\ info$ one can get information about her/his software and hardware

Get machine info Ctrl+I

Softare Information Ha	ardware Information	
	Software information	
Operating system: Linu	x Ubuntu 13.10 3.11.0-23-generic (64 bit 🏼 🎝
Cryptographic library:	OpenSSL 1.0.1e 11 Feb 2013	S
	🖌 ок	Q Cancel

Figure 1.4: Information about the operating system and used cryptographic library.

🛡 💿 QCM	Tool v 0.3.5 Machine Information	©
Softare Information	Hardware Information	
	Hardware information	
Processor(s): Intel(R) Core(TM) i7-3630QM CPU @ 2.40GH	z 🚺
Total memory:	15906 MB	000
	🖋 ок	🖉 Cancel

Figure 1.5: Information about the hardware of the machine on which *CMTool* was run.

4. Menu **Help**:



Figure 1.6: Information about the application.

- (a) Item **About** ... shows brief, general information about the *CMT* (SHIFT+A) (see Fig. 1.7)
- (b) Item **About the author** shows information about the author of the *CMT* (SHIFT+K) (see Fig. 1.8)
- (c) Item **CMTool's license** shows the CMTool's license text (SHIFT+L) (see Fig. 1.9)
- (d) Item Get some help shows this manual in a new window (CTRL+H)



Figure 1.7: Information about the application.



Figure 1.8: Information about the author.



Figure 1.9: *CMTool's* license.

When user selects some cryptographic primitives for benchmarking (it can be done by checking appropriate boxex in a scrolled check box located on the main window (see Fig. 1.10), then she/he needs to define some input parameters. One can define how many test she/he wants to run, how many iterations should be done in each test, how big (in bytes) input message for benchmarking primitive needs to be (see Fig. 1.12). User is also able to choose which type of operation she/he wants to run - one can choose between encryption and signing (or decryption/verifying respectively) (see Fig. 1.10, 1.11).



Figure 1.10: Choose some cryptographic primitives for benchmarking.



Figure 1.11: Choose operation type for benchmarking.

\odot	Crypto Metrics Tool v0.3.5	\odot \odot
e <u>L</u> anguage <u>I</u> nfo	Help	
😕 Benchmarking Para	meters JU Validation Parameters	
	Benchmarking input parameters	
Benchmark:	Encryption/Signing	✓ Tests: 10 ♦
Algorithms:	 	Lterations: 1000 🗘
Parallel benchmarks:	_	Input's size 1024 🗘
Number of parallel		1 🗘

Figure 1.12: Available benchmarking parameters.

Besides choosing the benchmarking parameters, user is able to set some validation parameters. She/he can chose the coefficient of variation (CV) value to determine if the results gathered by the CMT are the time series, and run the test with the specific confidence level. The validation process is performed according to the steps defined in the The robust measurement method for security metrics generation article.

\odot	Crypto Metrics Tool v0.3.5	\sim
e <u>L</u> anguage <u>I</u> nfo <u>H</u> elp		
Benchmarking Parameters	Validation Parameters	
	Validation input parameters	
Confidence Level (%):	80	v
Stationarity percent:		10 🛇

Figure 1.13: User can specify the *coefficient of variation* (CV) and the *confidence level* values.

Progress of performed tests can be seen at the progress bar located at the bottom of the CMTool's main window (see Fig. 1.14).

5)%
CMTOOL
Benchmarking AES/CBC with 128-bit key, this may take a while

Figure 1.14: Benchmarking progress can be seen on the progress bar.

When all benchmarking is done, final results are presented. One can see mean values for every tested cryptographic primitive (base measure) summarized in a table at the bottom of the main window (see Fig. 1.15).

By double-clicking each row of the CMTool's table with collected results (mean values), one is able to see more statistical information - mode, median, variance, standard deviation, kurtosis and skewness (see Fig. 1.16).

a Language Info	Help				
Benchmarking Parar	meters Validation	Parameters			
		Benchmarking in	put parameters		
Benchmark:	Encryption/Signing			✓ Tests:	10 🗘
Algorithms:	RC4-256 AES-CBC-128 AES-CBC-192			lterat	ions: 1000 🗘
Parallel benchmarks:	3			Input' Ibytes	s size 1024 🗘
Number of parallel					1 🗘
benchmarks:					
benchmarks: Stat	istics - below are just (mean values, double-cl	ick each row to see m	ore statistical inform	ation
benchmarks: Stat	istics - below are just i	mean values, double-cl	ick each row to see m	ore statistical inform	ation Cycles/Byte
benchmarks: Stat Algorithm MD4	istics - below are just (Speed [MB/s] 914.241	mean values, double-cl Wall time [ms] 0.00106022	ick each row to see m CPU time [ms] 0.000902333	ore statistical inform Calls/s 936182	ation Cycles/Byte 2.43318
benchmarks: Stat Algorithm MD4 AES/CBC (128-bit	istics - below are just i Speed [MB/s] 914.241 125.048	Wean values, double-cl Wall time [ms] 0.00106022 0.0077235	ick each row to see m CPU time [ms] 0.000902333 0.00768978	ore statistical inform Calls/s 936182 128049	etion Cycles/Byte 2.43318 17.9222
Algorithm MD4 AES/CBC (128-bit	istics - below are just i Speed [MB/s] 914.241 125.048	mean values, double-cl Wall time [ms] 0.00106022 0.0077235	CPU time [ms]	Cally's Cally's 936182 128049 Benchm	etion Cycles/Byte 2.43318 17.9222
Stat Algorithm MD4 AES/CBC (128-bit	istics - below are just i Speed [MB/s] 914.241 125.048	mean values, double-cl Wall time [ms] 0.00106022 0.0077235	CPU time [ms]	Calls/s Calls/s 936182 128049 Benchm	etion Cycles/Byte 2.43318 17.9222 nark Cancel

Figure 1.15: When the benchmarking is done, final results are presented.

aila	•	AES/CBC (12	B-bit key) Encrypti	on statistical info	rmation	
Г		Speed [MB/s]	Wall time [ms]	CPU time [ms]	Calls/s	Cycles/Byte
1	Variance	0.835751	3.18225e-09	1.34884e-09	876348	0.0319702
2	StdDev	0.914194	5.64114e-05	3.67266e-05	936.135	0.178802
3	Median	125.022	0.007699	0.007681	128023	17.9383
4	Mode	123.147	0.007652	0.007625	126103	17.6347
5	Skewness	-0.784025	0.306358	0.246362	-0.784025	0.113933
6	Kurtosis	2.61593	1.47067	2.57184	2.61593	2.13657

Figure 1.16: Measurement results are obtained, validated and presented to the user as statistical primitives.

CMTool's Installation Guide

2.1 Installation Guide for GNU/Linux-like Operating Systems

This chapter provides information about the installation of CMTool (simply, CMT) in console, as well as in GUI version on GNU/Linux-like operating systems.

2.1.1 CMTool Console Version - Installation

Example installation of CMT's console version was performed on Linux Mint 16 Petra and Fedora Linux 20 Heisenbug.

Installing CMT on Linux Mint 16 Petra



 \mathcal{Z}

For GNU/Linux like operating systems, console version of CMT is shipped as a source package which you need to compile by yourself.

1. Download *CMT's* source package (*.zip) from QoP-ML's webpage:

cd ~ wget http://qopml.org/wp-content/uploads/CMT/v0.3.5/CMT_V.3.5_LIN_CON_SRC.zip unzip CMT_V.3.5_LIN_CON_SRC.zip

					katie : bash – Konsole	\odot	\diamond	×	1
File	Edit	View	Bookmarks	Settings	Help				I
katie@)vm:~	> wget	http://qopml	.org/wp-c	ontent/uploads/CMT/v0.3.5/CMT_V.3.5_LIN_CON_SRC.zip			ĉ	ł

kat 🖾 💿	e : bash – Konsole 💿 💿 🛞
File Edit View Bookmarks Settings Help	
<pre>katie@vm:~ > unzip CMT_V.3.5_LIN_CON_SRC.zip</pre>	<u>^</u>

	katie : bash – Konsole	\odot \odot
File Edit View Bookmarks	Settings Help	
inflating: CMT_V.3.5_LIN_COM inflating: CMT_V.3.5_LIN_COM	_SRC/testsuite/test_block_ciphers_cfb.h _SRC/testsuite/test_block_ciphers_cfb.c _SRC/testsuite/test_test_block_ciphers_ecb.h _SRC/testsuite/test_rsa.c _SRC/testsuite/test_rsa.h _SRC/testsuite/test_module.c _SRC/testsuite/test_diffie_hellman.h _SRC/testsuite/test_block_ciphers_ge.c _SRC/testsuite/test_block_ciphers_ecb.c _SRC/testsuite/test_digital_signatures.h _SRC/testsuite/test_digital_signatures.c _SRC/testsuite/test_block_ciphers_ge.h _SRC/testsuite/test_block_ciphers_ge.h _SRC/testsuite/test_digital_signatures.h _SRC/testsuite/test_block_ciphers_ge.h _SRC/testsuite/test_block_ciphers_ge.h _SRC/testsuite/test_block_ciphers_ge.h _SRC/testsuite/test_digest.c	
atie@vm:~ >	_SKL/TESTSUITE/TEST_OITTIE_NELLMAN.C	
📔 🛛 kat	e : bash	

2. Since *CMT* uses *OpenSSL* for it's crypto benchmarks, to be able to compile and later use *CMT*, you should first install libssl-dev package. Libssl-dev is a part of the OpenSSL implementation of SSL, containing SSL development libraries, header files and documentation.

sudo apt-get install libssl-dev

Downloads : bash – Konsole	
File Edit View Bookmarks Settings Help	
katie@vm:~/Downloads > sudo apt-get install libssl-dev	<u>^</u>

3. *CMT*, as written in C/C++ languages, needs a C and C++ compilers to build executable files. Both gcc and g++ will do the perfect job:

```
sudo apt-get install gcc
sudo apt-get install g++
```

CMTool Manual Version 0.3.5, Copyright ©2014, Katarzyna Mazur, All rights reserved CMTOOL

	Downloads : bash – Konsole	\odot \otimes \otimes
File Edit View Bookmarks Settings Help		
atie@vm:~/Downloads > sudo apt-get install g	cc	^
	Downloads : bash - Konsole	
∎ ⊚ File Edit View Bookmarks Settings Help	Downloads : bash – Konsole	\odot \odot \otimes

4. To perform compilation process in a a smooth and easy way, using single command from Makefile delivered along with *CMT*, install build-essential package. Build-essential package contains tools (like the gcc compiler, make tool, etc.) for compiling/building software from source.

sudo apt-get install build-essentials

	Downloads : bash – Konsole	$\odot \odot \otimes$
File Edit	View Bookmarks Settings Help	
katie@vm:~/Do	ownloads > sudo apt-get install build-essential	<u>^</u>

5. After installing all the required components to build CMT, you can actually compile it. Simply cd to the directory where you unpacked CMT's source (unpacking CMT, we assumed your home/ directory):

CMT_V.3.5_LIN_CON_SRC : bash - Konsole	$\otimes \otimes \otimes$
File Edit View Bookmarks Settings Help	
<pre>katie@vm:~ > cd CMT_V.3.5_LIN_CON_SRC/ katie@vm:~/CMT_V.3.5_LIN_CON_SRC > ls CMTOOL.cpp common core docs info Makefile statistics testsuite validations katie@vm:~/CMT_V.3.5_LIN_CON_SRC ></pre>	Î

6. Now simply type make run to compile and link CMT:

ſ)				CMT_V.3.5_LIN_CON_SRC : bash – Konsole	
l	File	Edit	View	Bookmarks	Settings	Help	
l	katie(@vm:~/	CMT_V.3	B.5_LIN_CON_	SRC > make	run	<u>^</u>

7. Below you can see the compilation process:

CMT_V.3.5_LIN_CON_SRC : make - Konsole	$\odot \odot \otimes$
File Edit View Bookmarks Settings Help	
katie@vm:~/CMT_V.3.5_LIN_CON_SRC > make run g++ -ggdb -fopempp -g -c -Wall -ansi -pedantic CMTool.cpp gcc -ggdb -c -o core/benchmarking.o core/benchmarking.c	Î

CMTool Manual Version 0.3.5, Copyright ©2014, Katarzyna Mazur, All rights reserved CMTOOL 8. Compilation finished with no errors, meaning CMT has been successfully compiled and it is now ready to run (see Fig. 2.1).



Figure 2.1: Do not be afraid about the make: *** [run] Error 255 error, it is even not a real, actual error. It showed up because we ran (using the make run command) *CMT* without required parameters.

Installing CMT on Fedora 20 Heisenbug



For GNU/Linux like operating systems, console version of CMT is shipped as a source package which you need to compile by yourself.

1. Download *CMT's* source package (*.zip) from QoP-ML's webpage:

cd ~ wget http://qopml.org/wp-content/uploads/CMT/v0.3.5/CMT_V.3.5_LIN_CON_SRC.zip unzip CMT_V.3.5_LIN_CON_SRC.zip

2. Then, acquire root privileges:

su -

÷	root@localhost:~	-	•	×
File Edit Tabs Help				
[katie@localhost ~]\$ su - Password: [root@localhost ~]# 📕				

3. Since *CMT* uses *OpenSSL* for it's crypto benchmarks, to be able to compile and later use *CMT*, you should first install **Openssl-devel** package. **openssl-devel** is a part of the OpenSSL implementation of SSL, containing SSL development libraries, header files and documentation.

yum install openssl-devel



4. *CMT*, as written in C/C++ languages, needs a C and C++ compilers to build executable files. Both gcc and g++ will do the perfect job:

yum install gcc
yum install gcc-c++

CMTool Manual Version 0.3.5, Copyright ©2014, Katarzyna Mazur, All rights reserved CMTOOL



5. To perform compilation process in a a smooth and easy way, using single command from Makefile delivered along with *CMT*, install a group of Development Tools packages. Development Tools packages contain tools (like the gcc compiler, make tool, etc.) for compiling/building software from source. The Development Tools are a yum group, which is a predefined bundle of software that can be installed at once, instead of having to install each application separately. The Development Tools will allow you to build and compile software from source code.



6. After installing all the required components to build *CMT*, you can actually compile it. Simply cd to the directory where you unpacked *CMT's* source (unpacking *CMT*, we assumed your home/ directory):

Ŧ	katie@localhost:~/CMT_V.3.5_LIN_CON_SRC	- • ×
File Edit T	īabs Help	
[katie@loca [katie@loca CMTool.cpp	alhost ~]\$ cd CMT V.3.5_LIN_CON_SRC/ alhost CMT_V.3.5_LIN_CON_SRC]\$ [s core info statistics validations	
common	docs Makefile testsuite	
[katie@loca	alhost CMT_V.3.5_LIN_CON_SRC]\$	

7. Now simply type make run to compile and link CMT:



8. Compilation finished with no errors, meaning CMT has been successfully compiled and it is now ready to run (see Fig. 2.2).



Figure 2.2: Do not be afraid about the make: *** [run] Error 255 error, it is even not a real, actual error. It showed up because we ran (using the make run command) *CMT* without required parameters.

2.1.2 CMTool GUI Version - Installation

For GNU/Linux like operating systems, GUI version of CMT is shipped as a source package which you need to compile by yourself.

Installing CMT on Linux Mint 16 Petra



1. Simply download *CMT* from QoP-ML's webpage:

cd ~
wget http://qopml.org/wp-content/uploads/CMT/v0.3.5/CMT_V.3.5_LIN_GUI_SRC.zip
unzip CMT_V.3.5_LIN_GUI_SRC.zip

2. Since *CMT* uses *OpenSSL* for it's crypto benchmarks, to be able to compile and later use *CMT*, you should first install libssl-dev package. Libssl-dev is a part of the OpenSSL implementation of SSL, containing SSL development libraries, header files and documentation.

sudo apt-get install libssl-dev

ſ)				Downloads : bash – Konsole	$\odot \odot \odot$
l	File	Edit	View	Bookmarks	Settings	Help	
l	katie@	<u>ð</u> vm∶~/	Downloa	ids > sudo ap	ot-get ins	all libssl-dev	â

3. *CMT*, as written in C/C++ languages, needs a C and C++ compilers to build executable files. Both gcc and g++ will do the perfect job:

sudo apt-get install gcc
sudo apt-get install g++

0					Downloads : bash – Konsole	
File Edi	t View	Bookmarks	Settings	Help		
katie@vm:	-/Downloa	ads > sudo ap	ot-get ins	tall gcc		1

)					Downloads : bash – Konsole	
File	Edit	View	Bookmarks	Settings	Help		
katie	@vm:~/	Downloa	ads > sudo ap	ot-get ins	tall g++		Â

4. To perform compilation process in a a smooth and easy way, using single command from Makefile delivered along with *CMT*, install build-essential package. Build-essential package contains tools (like the gcc compiler, make tool, etc.) for compiling/building software from source.

sudo apt-get install build-essentials

ſ	Downloads : bash – Konsole	$\odot \odot \otimes$
l	File Edit View Bookmarks Settings Help	
I	katie@vm:~/Downloads > sudo apt-get install build-essential	<u>^</u>

5. Install libglu1-mesa-dev package. The libglu1-mesa-dev package includes headers and static libraries for compiling programs with GLU. For a complete description of GLU, please look at the libglu1-mesa package.

	•					Downloads : bash – Konsole	$\odot \odot \otimes$
Þ	File	Edit	View	Bookmarks	Settings	Help	
k	atie@)vm:~/I	Downloa	ids > sudo ap	ot-get ins	tall libglu1-mesa-dev -y	Â

6. Download Qt libraries. The easiest and the fastest way of doing this is to download QtCreator:

File Edit View History	/ <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp
👥 Download Qt Qt Proj	ect 🗣
qt-project.org/de	ownloads 🖓 🗸 😨
🔄 Most Visited 🗸 🛛 🖳 Lir	nux Mint 👅 Community 🐚 Forums 🐚 Blog 🛛 🔝 News 🗸
Dowmoad	λ QL
LO1	Qt is available under GPL v3, LGPL v2 and a commercial license. Learn more about licenses here. Developing with Qt professionally?
	Commercial license of QC offers more flexible licensing terms compared to the LGPL, additional modules, and includes support ensuring that someone is there for you if you need help. Please contact Digia for details.
	 Evaluate Qt under a commercial license (qt.digia.com)
O+ 5 3 0 (Onon Source
Qt 5.3.0 (Jpen Source
Suggested	download based on your operating system (UNIX):
We are guessing	you are running Firefox on Linux.
🕘 <u>Qt Online In</u>	Istaller for Linux 32-bit (23 MB) (Info)
Ot Online In	staller for Linux 64-bi of Online Installer for Linux 32 bit
•	
Not the version y	/ou wanted?
Show Download	s
ownload.qt-project.org/of	ficial_releases/online_installers/qt-opensource-linux-x86-1.6.0-3-online.run
_	
	🕽 😡 Opening qt-opensource-linux-x86-1.6.0-3-online.run 🕑 💿 🛞
	♥ ○ Opening qt-opensource-linux-x86-1.6.0-3-online.run ⊗ ⊗ ⊗ You have chosen to open:
	Opening qt-opensource-linux-x86-1.6.0-3-online.run You have chosen to open: Image: state stat
	 ✓ Opening qt-opensource-linux-x86-1.6.0-3-online.run ⊗ ⊗ ⊗ You have chosen to open: If qt-opensource-linux-x86-1.6.0-3-online.run which is: BIN file (22,8 MB) from: http://tto.fau. de
	 ✓ Opening qt-opensource-linux-x86-1.6.0-3-online.run ✓ ✓

7. Install Qt. Make the installer file executable by typing:

chmod u+x qt-opensource-linux-x86-1.6.0-3-online.run

	Downloads : bash – Konsole 💿 🛞
File Edit View Bookmarks Settings Help	
<pre>vm Downloads # chmod u+x qt-opensource-linux-x86- vm Downloads #</pre>	1.6.0-3-online.run ^

CMTool Manual Version 0.3.5, Copyright ©2014, Katarzyna Mazur, All rights reserved CMTOOL 8. Run the installer as the root user and simply install QtCreator:

)				Downloads : bash – Konsole	$\odot \odot \otimes$
File	Edit	View	Bookmarks	Settings	Help	
vm Dow	nload	s # ./o	t-opensource	e-linux-x8	-1.6.0-3-online.run	<u>^</u>

9. Extract *CMT*'s archive:

)					katie : bash – Konsole	\odot \odot \otimes
File	Edit	View	Bookmarks	Settings	Help		
katie(∂vm:~ :	> unzip	CMT_V.3.5_L	IN_GUI_SR	C.zip		Â

10. Go to the directory where you extracted CMT:

)				CMT_V.3	.5_LIN_GUI_SRC : bash – Kon	sole		\odot (∿ ⊗
File	Edit	View	Bookmarks	Settings	Help					
katie katie cmtoo commo katie	@vm:~; @vm:~/(l gui n icou @vm:~/(> cd CM CMT_V.3 .pro i ns i CMT_V.3	T_V.3.5_LIN .5_LIN_GUI mages.qrc .nfo .5_LIN_GUI	N_GUI_SRC/ SRC > ls main.cpp Makefile SRC > ■	QCMTool.cpp QCMTool.h	QCryptoBenchThread.cpp QCryptoBenchThread.h	QCryptoStats.cpp QCryptoStats.h	QInputParameters. QInputParameters.	cpp h	Î

11. Type make to compile CMT from source:

	0					CMT_V.3.5_LIN_GUI_SRC : bash – Konsole	
E F	ile	Edit	View	Bookmarks	Settings	Help	
ka	tie@	vm:~/	CMT_V.3	.5_LIN_GUI_	SRC > make		<u>^</u>

12. Type ./QCMTool to actually run CMT in gui mode:

ſ)				CMT_V.3.5_LIN_GUI_SRC : bash – Konsole	<u>> «</u>	ฦ
L	File	Edit	View	Bookmarks	Settings	Help		
L	katie(@vm:~/	CMT_V.3	.5_LIN_GUI_	SRC > ./QC	MTool	1	<u>^</u>

13. Alternatively, if you have any problems, install:

sudo apt-get install qt5-default

and then try to compile CMT (by typing make in the directory where you extracted CMT).

1	0					CMT_V.3.5_LIN_GUI_SRC : bash – Konsole	\odot	\odot \otimes
	File	Edit	View	Bookmarks	Settings	Help		
	katie@	vm:~/	CMT_V.3	3.5_LIN_GUI_	SRC > sudo	apt-get install qt5-default		Â

CMTool Manual Version 0.3.5, Copyright ©2014, Katarzyna Mazur, All rights reserved CMTOOL This package (qt5-default) sets Qt 5 to be the default Qt version to be used when using development binaries like qmake. It provides a default configuration for qtchooser, but does not prevent alternative Qt installations from being used.

2.2 Installation Guide for Microsoft Windowslike Operating Systems

This chapter provides information about the installation of CMTool (simply, CMT) in console, as well as in GUI version on Microsoft Windows-like operating systems. Installation was performed on Microsoft Windows Server 2012.

2.2.1 CMTool Console Version - Installation

Installing CMT on Windows Server 2012



For Microsoft Windows-like operating systems, CMT is shipped as an executable application, so you do not actually need to install it.

- 1. Simply download *CMT* from QoP-ML's webpage.
- 2. Extract CMT's archive:

😼 l 💽 🛄 👳 l		Compressed Folder Tools	Downloads	_ D X
File Home Share	View	Extract		~ ?
🄄 🕘 🔻 🚺 🕨 Ad	ministrator	Downloads	v 🖒 Search Download	s p
🔆 Favorites	Name	^	Date modified Type	Size
 Desktop Downloads Recent places Libraries Documents Music Pictures Videos Computer Local Disk (C:) Network 	<u>і</u> смт.	V.3.5_WIN_CON_BIN	Open Open Open in new window Pin to Start Extract All Open with Share with Restore previous versions Send to Cut Copy Create shortcut Delete Rename Properties	1,162 KB
1 item 1 item selected 1.	13 MB			:==

🏭 l ⊋ 👪 👳 l	CMT_V.3.5_WIN_CO	ON_BIN		_ D X
File Home Share	View			× 🕐
🔄 🍥 🔻 🕆 퉬 « CN	MT_V.3.5_WIN_CON_BIN ► CMT_V.3.5_WIN_CON	_BIN ∨ Ċ	Search CMT_V.3.5	5_WIN_CON 🔎
🔆 Favorites	Name	Date modified	Туре	Size
Desktop	CMTool	6/17/2014 12:20 PM	Application	257 KB
🗼 Downloads	iibeay32.dll k≷	6/17/2014 12:20 PM	Application extens	1,130 KB
📃 Recent places	🚳 msvcp100.dll	6/17/2014 12:20 PM	Application extens	412 KB
	🚳 msvcr100.dll	6/17/2014 12:20 PM	Application extens	756 KB
🥽 Libraries	🚳 vcomp100.dll	6/17/2014 12:20 PM	Application extens	50 KB
Documents				
J Music				
Pictures				
yideos				
🖳 Computer				
📥 Local Disk (C:)				
🙀 Network				
5 items				:==

Open up cmd.exe and cd to the location, where you extracted *CMTool*:



C14.	Administrator: Command Prompt		ĸ
C:\Users\Ad Volume in Volume Ser	lministrator∖Downloads\CMT_U.3.5_WIN_CON_BIN>dir driue C has no label. ∙ial Number is 0637-A0FF		Â
Directory	of C:\Users\Administrator\Downloads\CMT_U.3.5_WIN_CON_BIN	l	
96/17/2014 96/17/2014 96/17/2014 96/17/2014 96/17/2014 96/17/2014 96/17/2014	12:20 PM (DIR) 12:20 PM (DIR) 12:20 PM 263,168 CMTool.exe 12:20 PM 1,157,120 libeay32.dll 12:20 PM 421,200 msvcpi00.dll 12:20 PM 773,968 msvcpi00.dll 12:20 PM 773,968 msvcpi00.dll 12:20 PM 51,024 vcompi00.dll 5 File(s) 2,666,480 bytes 2 Dir(s) 6,140,555,264 bytes free Hoisistwatow Downloads/CMT 4,25 UNN CON PIN)	k	
01-0321-S (nt			×

3. Run *CMT* by typing CMTool.exe:



2.2.2 CMTool GUI Version - Installation

For Microsoft Windows-like operating systems, CMT is shipped as an executable application, so you do not actually need to install it.

Installing CMT on Windows Server 2012



- 1. Simply download CMT from QoP-ML's webpage.
- 2. Extract *CMT*'s archive:



🌡 l ⊋ 🖺 = I	Application	Tools	CMT_V.3.5_WIN_G	UI_BIN	_ 🗆 X
File Home Share	View Manag	e			× 🔞
€ 🗇 ▼ ↑ 퉲 « CM	IT_V.3.5_WIN_GUI_BIN ►	CMT_V.3.5_WIN_GUI_BI	N► v Č	Search CMT_V.3.5	5_WIN_GUI_B 🔎
🔆 Favorites	Name	•	Date modified	Туре	Size
Desktop	imageformats		6/17/2014 10:54 AM	File folder	
🐌 Downloads	platforms		6/17/2014 12:08 AM	File folder	
📃 Recent places	🚳 icudt51.dll		6/17/2014 10:54 AM	Application extens	21,794 KB
	🚳 icuin51.dll		6/17/2014 10:54 AM	Application extens	1,726 KB
🥽 Libraries	🚳 icuuc51.dll		6/17/2014 10:54 AM	Application extens	1,266 KB
Documents	🚳 libeay32.dll		6/17/2014 10:54 AM	Application extens	1,130 KB
🎝 Music	🚳 libEGL.dll		6/17/2014 10:54 AM	Application extens	47 KB
Pictures	libGLESv2.dll		6/17/2014 10:54 AM	Application extens	712 KB
🛃 Videos	🚳 msvcp100.dll		6/17/2014 10:54 AM	Application extens	412 KB
	🚳 msvcr100.dll		6/17/2014 10:54 AM	Application extens	756 KB
🖳 Computer	🕀 QCMTool	Ν	6/17/2014 10:54 AM	Application	389 KB
🏜 Local Disk (C:)	Qt5Core.dll	Date created: 6/17/2014	6/17/2014 10:54 AM	Application extens	3,767 KB
	🚳 Qt5Gui.dll	Size: 388 KB	10:54 AM	Application extens	2,857 KB
📬 Network	Qt5Network.dll		6/17/2014 10:54 AM	Application extens	807 KB
	🗟 Qt5OpenGL.dll		6/17/2014 10:54 AM	Application extens	238 KB
	Qt5PrintSupport.d	II	6/17/2014 10:54 AM	Application extens	221 KB
	Qt5Qml.dll		6/17/2014 10:54 AM	Application extens	1,517 KB
	Qt5Quick.dll		6/17/2014 10:54 AM	Application extens	1,887 KB
	Qt5Sql.dll		6/17/2014 10:54 AM	Application extens	147 KB
	Qt5WebKitWidgets	s.dll	6/17/2014 10:54 AM	Application extens	177 KB
	Qt5Widgets.dll		6/17/2014 10:54 AM	Application extens	4,172 KB
21 items 1 item selected	388 KB				

3. Run *CMT* by double-clicking *CMTool's* icon:

CMTool's Screenshoots

3

CMTool is available for GNU/Linux and Microsoft Windows operating systems. Supported operating system list includes (but it is not limited to):

- Ubuntu, Kubuntu, Xubuntu, Lubuntu, Debian, ...
- Linux Mint
- Fedora
- OpenSUSE
- CentOS
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8

Below are some screenshots of the *CMTool*. One can see how *CMTool's* interface looks on supported operating systems.

Longuogo Into I	Crypto Metrics Tool v0.3.5	0
Language into i		
Benchmarking Pai	rameters Jalidation Parameters	
enchmarking input	parameters	
Benchmark:	Encryption/Signing Tests: 0	
Al	All MD4	
Algorithms:	SHA-1	1
Parallel benchmark	s: Input's size 0	a.
Number of parallel		1
benchmarks:	- IV	
ietice - below are ius	t mean values, double-click each row to see more statistical information	
stics - below are jus	a mean values, double-click each row to see more statistical mormation	
		-
	Banabmark	
	Benchmark	_
	0%	
	0% CMTC	
	0% CMTC	DC
o Metrics Tool v0.3.5	0% 5 is ready to go	C
o Metrics Tool v0.3.	0% CMTC	C
o Metrics Tool v0.3.	0% CMTC	DC
to Metrics Tool v0.3.3	0% CMTC	C
o Metrics Tool v0.3.	O% CMTc O% CMTc Software information Software information Software information	C
o Metrics Tool v0.3.	O% CMTC O% CMTC Softare Information Hardware Information Software Information Software Information Decrafting system: Linux Ubuntu 13.10.23-generic 64 bit	C
o Metrics Tool v0.3.	Benchmark Cancel 0% CMTC 5 is ready to go Software information Software information Hardware information Software information Hardware information Software information Genetic formation Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Construerable library Operating 1.11 feb 2013	C
o Metrics Tool v0.3.	O% O% CMTC 5 is ready to go Softare Information Softare Information Software information Hardware Information Software information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit OperSSL 1.0.1e 11 Feb 2013	C
:o Metrics Tool v0.3.	Benchmark Cancel 0% CMTC 5 is ready to go Software information Software information Hardware Information Software information Hardware Information Software information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OpenSSL 1.0.1e 11 Feb 2013	C
to Metrics Tool v0.3.	0% 0% CMTC 5 is ready to go Software information Hardware information Software information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OpenSSL 1.0.1e 11 Feb 2013 OK Cancel	
to Metrics Tool v0.3.	O% O% CMTC 5 is ready to go Softare Information Hardware Information Software Information Hardware Information Software Information Unux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OpenSSL 1.0.1e 11 Feb 2013 OK Cancel	DC
o Metrics Tool v0.3.	O% O% CMTC 5 is ready to go Software information Software information Hardware information Software information Hardware information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OK Cancel	C
o Metrics Tool v0.3.	O% CMTC 5 is ready to go Softare Information Very Control v 0.3.5 Machine Information Software Information Hardware Information Software Information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OK Cancel	
:o Metrics Tool v0.3.	Benchmark Cancel 0% CMTC 5 is ready to go Softare Information Softare Information Software Information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OpenSSL 1.0.1e 11 Feb 2013 OK Cancel	DC
co Metrics Tool v0.3.	Benchmark Cancel 0% CMTC 5 is ready to go Operating system: Unux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: Operating system: Unux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OK Cancel	
:o Metrics Tool v0.3.	O% CMTC Soft ready to go Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Operating system: Unux Ubuntu 13.10 3.11.0-23-generic 64 bit OK Cancel OK Cancel	
co Metrics Tool v0.3.	O% CMTC 5 is ready to go Operating system: Unux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: Operating system: Unux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OK Cancel	
co Metrics Tool v0.3.	0% CMTC 0% Software information Very Control v 0.3.5 Machine information Software information Hardware information Operating system: Linux Ubuntu 13.10 3.11.0-23-generic 64 bit Cryptographic library: OpenSSL 1.0.1e 11 Feb 2013 OK Cancel	

Figure 3.1: CMTool on Kubuntu 13.10 4 LTS, 64 bit.

Language Info H	alp		
Benchmarking Parame	ters J Validation Parameters		
enchmarking input pa	rameters		
Benchmark:	Encryption/Signing	Cartests:	o
Algorithms:	□ All □ MD4	terations:	0
Parallel benchmarks:		Input's size [bytes]:	0
Number of parallel benchmarks: istics – below are just	mean values, double-click each row to	o see more statistical informat	1 💭
Number of parallel benchmarks: istics – below are just	mean values, double-click each row to	• see more statistical informat	ion
Number of parallel benchmarks: istics – below are just	mean values, double-click each row to	see more statistical informat	1

GCM	
Softare Information	Hardware Information
Software information	n
Operating system:	Linux 3.2.0-4-amd64 64 bit 🛛 🐧
Cryptographic libr	ary: OpenSSL 1.0.1e 11 Feb 2013 🔗
	Cancel OK
QCM	iool v 0.3.5 Machine Information
QCM [*] Softare Information	Tool v 0.3.5 Machine Information
QCM ⁻ Softare Information Hardware informatior	Tool v 0.3.5 Machine Information
QCM ⁻ Softare Information Hardware informatior Processor(s) : Inte	Tool v 0.3.5 Machine Information Hardware Information (R) Core(TM) i7-3630QM CPU @ 2.40GHz
QCM Softare Information Hardware informatior Processor(s): Inte Total memory:	Cool v 0.3.5 Machine Information Hardware Information (R) Core(TM) i7-3630QM CPU @ 2.40GHz 1002 MB

Figure 3.2: *CMTool* on Debian Wheezy 7, 32 bit.

Lawrence Juda II.		
Language Info H	elp	
Benchmarking Para	meters Validation Parameters	
nchmarking input par	ameters	
2		
Benchmark:	Encryption/Signing	Tests: 0
		A
Algorithms:	MD4 MD5	Iterations: 0
	SHA-1 SHA-224	-
Parallel benchmarks:		Input's size
a and benefitiand the		[bytes]:
Number of parallel benchmarks:		1
tics - below are just n	ean values, double-click each row to see more statistical inform	nation
tics - below are just n	ean values, double-click each row to see more statistical inform	nation
tics - below are just n	ean values, double-click each row to see more statistical inform	nation Benchmark Cancel
tics - below are just n	ean values, double-click each row to see more statistical inform	nation Benchmark Cancel
tics - below are just n	nean values, double-click each row to see more statistical inform	nation Benchmark Cancel



	quinton robbs machine anormation	
Softare Informat	ion Hardware Information	
Hardware informat	tion	
Processor(s):	Intel(R) Core(TM) i7-3630QM CPU @ 2.40GHz	
Total memory:	1002 MB	000

Figure 3.3: *CMTool* on Linux Mint 16 32 bit.

🔶 Crypto Me	etrics Tool	v0.3.5
File Language	e Info ⊦	elp
😕 Benchn	marking Parar	neters Validation Parameters
Benchmar	rking input pa	rameters
Benchmar	ırk:	Encryption/Signing
Algorithm	ns:	MD4 MD5
		SHA-1 SHA-224
Parallel b	enchmarks;	Input's size
Number	-6 -	[bytes]:
benchma	or parallel irks:	1 .
Statistics - be	elow are just i	nean values, double-click each row to see more statistical information
[0%
		CMTOOL
Crypto Metrics T	Tool v0.3.5 is	ready to go 🧰
		QCMTool v 0.3.5 Machine Information
		😻 Softare Information 🛛 📜 Hardware Information
		Software information
		Operating system: Microsoft Windows XP Professional 5 1 32-bit
		Cryptographic library: OpenSSL 1.0.1e 11 Peb 2013
		OK Cancel
	_	
	2	QCMTool v 0.3.5 Machine Information
		😻 Softare Information 🛛 🐫 Hardware Information
		Hardware information
		Processor(s): Intel(R) Core(TM) i7-36300M CPU @ 2,40GHz
		Total memory 1022 MP
		OK Cancel

Figure 3.4: CMTool on Microsoft Windows XP, 32 bit.



Figure 3.5: *CMTool* on Microsoft Windows 7, 32 bit.