# MantaRay Documentation

*Release 1.3.8*

Douglas Koster, Kevin Murphy, Chapin Bryce

Sep 27, 2017

# Contents

# CHAPTER 1

# About MantaRay

MantaRay was designed to automate processing forensic images, directories and individual files with open source tools. With support for numerous image formats, this tool provides a scalable base to utilize open source and custom exploitation tools. MantaRay was developed by two forensic analysts, Doug Koster and Kevin Murphy. With more than 25 years of collective experience in computer forensics, they have created a formidable program designed for the bulk automation of repetitive forensic processes. Utilizing the work of some of the great open source developers (in no particular order) such as Brian Carrier, Harlan Carvey, Simson Garfinkel, Kris Kendall, Jesse Kornblum, Nick Mikus, Kristinn Guðjóns and Joachim Metz the tool provides a one-stop shop of highly valuable tools. Additionally, the MantaRay team is working to provide new groundbreaking additions to these open source tools. The first of which is the automated registry recovery and processing tool.

ManTech was founded in 1968 to provide advanced technological services to the United States government. We began with a single contract with the U.S. Navy to develop war-gaming models for the submarine community. Over the years, our government's technology needs have increased dramatically in scope and sophistication, and we have grown to meet that challenge.

For more than 40 years, we kept a careful eye on where emerging technologies were taking the government, and we developed the resources to master those technologies—by staying close to our customers and anticipating their needs, hiring talented professionals to propel us into the future, and acquiring companies with proven capabilities.

Today, we are a $3 billion public company that provides the innovation, adaptability, and critical thinking our government needs for success in defense, intelligence, law enforcement, science, administration, and other fields throughout the nation and in many countries throughout the world. We are now applying the lessons learned in the unforgiving arena of national security to help the private sector protect networks and critical information.

Return to documentation home *MantaRay Documentation*

# CHAPTER 2

# Careers

ManTech offers challenging and rewarding work, generous benefits, and a commitment to help you grow professionally. If you are dedicated to your work, committed to learning and growing, and of good character, you will probably feel right at home with us. Find out why so many people are proud to work at ManTech and explore the opportunities we might have for you.

Please use the resources below to find and apply for positions:

ManTech Careers Home

Computer Forensic Jobs with ManTech

ManTech Positions with the Computer Forensic & Intrusion Analysis (CFIA) Division

Return to documentation home *MantaRay Documentation*

CHAPTER 3

# Contributors

## ManTech Development Team

Project Manager & Lead Programmer

Doug Koster
M.S. CS, MBA, A+, EnCE, PMP, GCFE, GCFA
Senior Computer Forensic Analyst
ManTech | Mission, Cyber & Intelligence Solutions Group

Lead Computer Forensic Analyst & Contributing Programmer

Kevin Murphy
Senior Computer Forensic Analyst, A+, EnCE
B.S., Computer and Digital Forensics
ManTech | Mission, Cyber & Intelligence Solutions Group

Contributing Programmer & Quality Assurance

Chapin Bryce
Senior Technical Intern, ACE
B.S., Computer and Digital Forensics (April, 2015)
ManTech | Mission, Cyber & Intelligence Solutions Group

## Graphic Design

Roger F. Gordon
Senior Illustrator
ManTech Corporate Design Solutions

## Forensic Script & Tool Contributors

BulkExtractor

- Simson Garfinkel, Bruce Allen, Alex Eubanks, Luis E. Garcia II, Michael Shick

ENT – Calculat Entropy

- John Walker, Wesley Landaker

KML from JPG EXIF Data

- Kyle Lancaster

fdupes

- Adrian Lopez – fdupes, Doug Koster

EXIF Tool

- Phil Harvey

Foremost

- Kris Kendall, Jesse Kornblum, Nick Mikus

Jumplist Parser

- Harlan Carvey

NTFS Arifact Extractor

- Douglas Koster, Kevin Murphy

Sleuth Kit tools

- Brian Carrier

Registry Hive Extractor (MantaRay)

- Douglas Koster, Kevin Murphy

Regripper

- Harlan Carvey

Super Timeline

- Kristinn Guðjóns

Volatility

- Mike Auty, Andrew Case, Michael Cohen, Brendan Dolan-Gavitt, Jamie Levy, Michael Ligh, AAron Walters

Return to documentation home *MantaRay Documentation*

CHAPTER 4

# MantaRay Forensics

ManTech Triage and Analysis System, Forensics Workflow Automation Suite

# CHAPTER 5

# Overview

MantaRay is designed to automate the processing of forensic images, directories and individual files with open source tools. With support for numerous image formats, this tool provides a scalable base to utilize open source and custom exploitation tools.

For more information about the suite, visit our website http://www.mantarayforensics.com

# CHAPTER 6

# Dependencies

See https://launchpad.net/~mantaray/+archive/stable for a full list

- BulkExtractor
- ENT – Calculate Entropy
- KML from JPG EXIF Data
- fdupes
- EXIF Tool
- Foremost
- Jumplist Parser
- Sleuth Kit tools
- Regripper
- Log2Timeline
- Volatility

# CHAPTER 7

# Installation of MantaRay

## PPA:

```
$ sudo apt-add-repository ppa:mantaray/stable
$ sudo apt-add-repository ppa:sift/stable
$ sudo apt-get update && sudo apt-get upgrade -y
$ sudo apt-get install mantaray
```

## Source from PPA:

```
$ sudo apt-add-repository ppa:mantaray/stable
$ apt-get source mantaray
```

## GitHub:

```
$ git clone https://github.com/mantarayforensics/mantaray.git
$ cd mantaray
```

Follow PPA directions to install dependencies

# CHAPTER 8

# How To Run MantaRay

From command line (as user with sudo privileges) in PPA:

```
$ sudo mantaray
```

A popup window should appear. Pressing continue will begin running the script.

CHAPTER 9

# Check For Updates

Using apt-get:

```
$ sudo apt-get update && sudo apt-get upgrade
```

Using mantaray-updater:

```
$ sudo mantaray-updater
```

GitHub:

```
$ git pull origin master
```

# CHAPTER 10

## Errors and Bugs

If MantaRay crashes, please re-run it in debug mode and send a screenshot of the crash along with any other details you can report to our GitHub https://github.com/mantarayforensics/mantaray/issues