CrowdsourcedDFIRBook

A crowdsourced DFIR book by members of the Digital Forensics Discord Server

Andrew Rathbun, ApexPredator and Kevin Pagano

CrowdsourcedDFIRBook

A crowdsourced DFIR book by members of the Digital Forensics Discord Server

Andrew Rathbun, ApexPredator and Kevin Pagano

This book is for sale at http://leanpub.com/crowdsourceddfirbook

This version was published on 2022-05-01

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

Introduction

TODO for Andrew

Markdown Example

Writing in Markdown is easy! You can learn most of what you need to know with just a few examples.

To make *italic text* you surround it with single asterisks. To make **bold text** you surround it with double asterisks.

Section One

You can start new sections by starting a line with two # signs and a space, and then typing your section title.

Sub-Section One

You can start new sub-sections by starting a line with three # signs and a space, and then typing your sub-section title.

Including a Chapter in the Sample Book

At the top of this file, you will also see a line at the top that says `{sample: true}`, immediately above the # Chapter Two title. This means that when you generate a preview of your book, or publish a new version of your book, this chapter will be included in a separate sample book that will be created. When you publish your book, this will give potential readers a sample book to read, when they are deciding whether they want to buy your book.

Links

You can add web links easily. Here is a link to the Leanpub homepage[1].

When you are creating a web link, the part between the square brackets [ ] contains the words that people will see in your book, and the part in the round brackets ( ) is the web address you are linking to.

Images

You can add an image to your book in a similar way.

First, add the image to the "resources" folder for your book. You will find the "resources" folder in your book's "manuscript" folder, which is at the top level of your book's folder in GitHub or Bitbucket.

If you look in your book's "resources" folder right now, you will see that there is an example image there with the file name "palm-trees.jpg". Here's how you can add this image to your book:

[1] https://leanpub.com

Palm Trees

As this example image shows, **on a line by itself** you type an exclamation point !, followed by the image caption between square brackets and the filename between round brackets.

To learn more about adding images, see this link[2].

Lists

Numbered Lists

You make a numbered list like this:

1. kale
2. carrot
3. ginger

[2] https://leanpub.com/markua/read#images

Bulleted Lists

You make a bulleted list like this:

- kale
- carrot
- ginger

Code Samples

You can add code samples really easily. Code can be in separate files (a “local” resource) or in the manuscript itself (an “inline” resource).

Local Code Samples

Here’s a local code resource:

Hello World in Ruby

```
1  puts "hello world"
```

Inline Code Samples

Inline code samples can either be spans or figures.

A span looks like `puts "hello world"` this.

A figure looks like this:

```
1  puts "hello"
```

You can also add a caption:

Hello World in Ruby

```ruby
puts "hello"
```

To learn more about adding code samples, see this link[3].

Tables

You can insert tables easily inline, using the GitHub Flavored Markdown (GFM) table syntax:

Header 1	Header 2
Content 1	Content 2
Content 3	Content 4 Can be Different Length

To learn more about adding tables, see this link[4].

Math

You can easily insert math equations inline using either spans or figures.

Here's one of the kinematic equations $d = v_i t + \frac{1}{2} a t^2$ inserted as a span inside a sentence.

Here's some math inserted as a figure.

[3] https://leanpub.com/markua/read#code
[4] https://leanpub.com/markua/read#tables

$$\left|\sum_{i=1}^{n} a_i b_i\right| \le \left(\sum_{i=1}^{n} a_i^2\right)^{1/2} \left(\sum_{i=1}^{n} b_i^2\right)^{1/2}$$

Something Involving Sums

To learn more about adding math, see this link[5].

How Book.txt Works

If you look in your book's "manuscript" folder, you will see there is a file called "Book.txt".

The "Book.txt" file is what our book generators use to decide what other files to include in your book. It is a list of the files in your "manuscript" folder that you decide you want to include in your book.

You can have multiple chapters in one file, but we recommend one chapter per file. This way, it's easier to navigate.

If you open the "Book.txt" file now, you will see the following list:

chapter1.txt
chapter2.txt
chapter3.docx
chapter4.docx

If you want to write in plain text, you should delete the following lines in the "Book.txt" file, and save the change:

chapter3.docx
chapter4.docx

(Those files are for people who want to write in Word, not in plain text.)

Now, the only two lines listed in the "Book.txt" file will be:

[5] https://leanpub.com/markua/read#math

chapter1.txt
chapter2.txt

The next time you create generate a preview of your book, our book generators will only use the "chapter1.txt" and the "chapter2.txt" files, because they are the only files listed in the "Book.txt" file. Our book generators will ignore any files in your "manuscript" folder that are not listed in the "Book.txt" file, even if those other files are still in the "manuscript" folder.

Creating a Preview of Your Book

You can generate a new version of your book any time by going to the "Preview" page for your book on Leanpub.

To go to the Preview page for your book, click on the Versions tab on Leanpub when you are working on your book. By default you will be taken to the "Preview New Version" page, which is where you'll be able to preview your book.

Getting Help

Finally, to get help, go to the Help tab for your book in Leanpub and then either…

1. See our Getting Started page to learn how to get started.
2. See our Getting Help page to learn how to get help.
3. Clicking the link to the Markua manual[6] on the Getting Help page. The Markua manual contains everything you need to know about writing in Markdown on Leanpub. (Our dialect of Markdown is called Markua.)

[6] https://leanpub.com/markua/read

By the way, that was how you make a numbered list in Markdown.

You can also make a bulleted list like this:

- item one
- the second item
- another item

We hope that you find writing in Markdown on Leanpub to be simple and enjoyable!

Authors

Author bios go here

History of the Digital Forensics Discord Server

Special thanks to Kevin Pagano for creating the logo for the Digital Forensics Discord Server!

History of the Digital Forensics Discord Server

I felt it was prudent to choose this topic for this project because very few others could provide as in depth of an account on the history of the Digital Forensics Discord Server. More to come in this section.

Beginnings in IRC

Long before the Digital Forensics Discord Server came to be, there existed a channel on an IRC[7] network called freenode[8]. The channel was called `#mobileforensics`. This channel had its humble beginnings on a Google Group ran by Bob Elder of TeelTech[9], called the Physical and RAW Mobile Forensics Group[10], which still exists today. In order to gain access to this Google Group, one had to have attended a TeelTech training in the past. It was, and continues to be, a phenomenal resource for those of us in Law Enforcement trying to navigate the waters of mobile forensic acquisitions.

By way of background, In February 2016 I attended the JTAG/Chip-Off class by TeelTech taught by Mike Boettcher and gained an invite to the Physical and RAW Mobile Forensics Group. I actively participated in the group to the extent my knowledge and curiosity enabled me. Make no mistake about, almost every other active poster in that group was more experienced or knowledgeable than myself. However, I thought to myself that there was no better place

[7] https://en.wikipedia.org/wiki/Internet_Relay_Chat
[8] https://en.wikipedia.org/wiki/Freenode
[9] https://www.teeltech.com/
[10] https://groups.google.com/g/physical-mobile-forensics/about?pli=1

to immerse myself in or people to surround myself with than this group if I wanted to be the best version of myself.

On August 23, 2016, a user that went by the name of `tupperwarez` had informed the group that they were starting an IRC channel called `#mobileforensics` in an effort "exchange ideas & have live discussions", as the post stated. I have been using forums for all of my internet life up until this point and I think subconsciously I was ready for something more, and this was it! I also knew that IRC was a longstanding tradition but I had never dabbled with it as I only had previous experience with messaging clients such as AOL Instant Messenger (AIM)[11] and MSN Messenger[12] at the time. 13 minutes after the post went out by `tupperwarez`, I was the first to respond in the thread that I had joined.

Throughout the next year and a half, a small contingent of people totaling anywhere from 7-15 at any given time occupied this IRC channel. We became a really tightknit group of examiners who relied on each other's knowledge and expertise to navigate challenges in our everyday casework. These problems often would relate to performing advanced acquisition methods using Chip-Off, JTAG, or flasher boxes. The collaboration was exactly what I was looking for because through each other we were able to cast a wider net for knowledge that we sought for problems we were coming across in our everyday investigations.

I recall utilizing an application called HexChat[13] to access this IRC channel. I'd have HexChat open at all times along with my everyday workflow of software applications to perform my duties as a Detective. For those reading this who have not used IRC before, know that's its nowhere near as feature rich as Discord. Discord is much more modern and IRC has been around since the "early days" of the internet as we know it today. I bring this up because often we needed to share pictures with each other as an exhibit for a problem

[11] https://en.wikipedia.org/wiki/AIM_(software)
[12] https://en.wikipedia.org/wiki/Windows_Live_Messenger
[13] https://hexchat.github.io/

we were encountering during the acquisition or decoding process of a mobile device.

Move to Discord

Truthfully, I had forgotten this detail I'm about to share but one of the moderators reminded me of it a couple of years ago and it all came back to me. One of the main catalysts for moving from IRC was the fact that I was really annoyed with having to upload a picture to imgur and share the link on the IRC channel as it seemed inefficient and the process grew stale for me. I had created a Discord account back in September 2016 to join various special interest servers so I had a fair amount of exposure to Discord's capabilities prior to the birthdate of the Digital Forensics Discord Server, which is March 26th, 2018.

I recall having aspirations for a move to Discord months prior to March 2018. For those who didn't use Discord around this time, it was primarily a platform marketed towards gamers. Using it for things other than gaming wasn't the intended purpose at the time, but the functionality it had was everything I wanted in a chat client. Take all of the good features from every other chat application I had used up until that point in time and add even more quality of life features and an awesome mobile application, and I was sold. I didn't like how it wasn't as seamless to use IRC on my phone and combined with the inefficient image uploading process, Discord was a breath of fresh air.

I was reminded that the major push to move to Discord came from me mostly surrounding the image uploading process combined with the positive experiences I had with the platform in my personal life via special interest servers from September 2016 to March 2018. The call to move to Discord was met with nearly unanimous approval from members of the IRC channel. As a result, the Mobile Forensics Discord Server was created!

Mobile Forensics Discord Server -> Digital Forensics Discord Server

The Mobile Forensics Discord Server enjoyed great success and rapid growth throughout its first year of existence. The server's growth was entirely driven by word of mouth and advertising on various Google Groups. The list of channels maintained in the server were driven by member requests which quickly expanded outside of mobile devices. Over time, it became increasingly apparent that branding the server as a Mobile Forensics server did not fully encompass the needs of the DFIR community. To the best of my research, the Mobile Forensics Discord Server was rebranded to the Digital Forensics Discord Server sometime around February 2019.

Since then, multiple channels have been added, renamed, and removed at the request of members.

Member Growth

Throughout the 4 years (as of this writing), the Digital Forensics Discord Server has undergone substantial growth. Below are some major membership milestones that were mined from Announcements I made in the `#announcements` channel over time.

Major Milestones

Date	# of Members
3/26/2018	3
3/29/2018	116
4/3/2018	142
4/6/2018	171
4/11/2018	200
4/13/2018	250
5/30/2018	300
6/28/2018	375
7/9/2018	400
7/25/2018	450
8/20/2018	500
9/27/2018	600
11/16/2018	700
12/6/2018	800
1/10/2019	900
2/1/2019	1000
5/8/2019	1500
10/4/2019	2000
1/30/2020	2500
3/27/2020	3000
5/22/2020	4000
3/26/2021	6800
8/2/2021	8000
1/29/2022	9000
3/26/2022	9500

Hosting the Magnet Virtual Summit 2020

In early 2020, shortly after the COVID-19 pandemic began, I was approached by representatives from Magnet Forensics inquiring about the possibility of providing a centralized location for attendees of the Magnet Virtual Summit 2020 to chat during presentations. Enthusiastically, we accepted the idea and began to plan the logistics of hosting what likely would become a large influx of

members. I seem to recall nearly 1500 members joining during the month long Magnet Virtual Summit 2020.

In retrospect, it's clear that this was one of the first indicators that the server had "made it" in the eyes of the community.

SANS DFIR Virtual Summit 2020 went virtual

Community Engagement Within the Server

vendors and customers

Impact on the DFIR community

solo cop up in alaska who's nearest fellow examiner is 3 hours away

Law Enforcement roles were separated by country from the early stages of the server for the purpose of delineating members from each other due to various legal considerations that may vary from one jurisdiction to another. Because of that, enumerating a list of the countries that a Law Enforcement role has been created for is likely the best way to establish the reach the Digital Forensics Discord Server has had on the DFIR community on a global level.

Countries with roles assigned for Law Enforcement personnel (as of May 2022):

- Albania
- Argentina
- Australia
- Austria
- Bangladesh
- Belgium

- Bosnia
- Brazil
- Canada
- Chile
- China
- Columbia
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Dominican Republic
- Estonia
- Finland
- France
- Germany
- Greece
- Grenada
- Iceland
- India
- Indonesia
- Iraq
- Ireland
- Israel
- Italy
- Jamaica
- Japan
- Korea
- Latvia
- Lithuania
- Luxembourg
- Maldives
- Malaysia
- Malta
- Mongolia

- New Zealand
- Mauritius
- Mexico
- Monaco
- Nepal
- Nigeria
- Norway
- Pakistan
- Netherlands
- Poland
- Portugal
- Romania
- Royal Cayman Islands
- Russia
- Senegal
- Seychelles
- Singapore
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Taiwan
- Turkey
- United Arab Emirates
- United Kingdom
- Ukraine
- Uruguay
- USA
- Vietnam

To save you from counting, that's 70 countries with a dedicated Law Enforcement role. This means that someone who has identified themselves as someone who works in Law Enforcement in one of

these countries has joined the server and had this role assigned to them. At least 1 person from each of these countries that at the time served in a Law Enforcement capacity have joined the Digital Forensics Discord Server. With 195 countries[14] recognized in the world as of the writing of this book, the server has a reach into approximately 36% of those!

Future

The Digital Forensics Discord Server will continue to live and thrive so long as the community wills it.

For those who are new to administering Discord servers, one important thing to know is that only the member who is assigned as the Server Owner can delete the server. Currently, that person is me, Andrew Rathbun. In the interest of ensuring the Digital Forensics Discord Server lives far beyond all of us (assuming Discord is still around by that time), I've established a paper trail for any other moderators to follow should anything happen to me to where I will never be able to log back in to Discord. This paper trail will require a lot of effort and coordination with family members/friends of mine to access my password vault and many other necessary items in order to Transfer Ownership[15] so that the server can live on without any administrative hiccups.

[14] https://www.worldatlas.com/articles/how-many-countries-are-in-the-world.html
[15] https://support.discord.com/hc/en-us/articles/216273938-How-do-I-transfer-server-ownership

Most Common Data Stores in Mobile Forensics

By Alexis Brignoni

Online presence: https://linqapp.com/abrignoni[16]

The Artisanal Approach

Most mobile forenisc examinations involve the use of third party tools to extract and decode information stored whitin targeted devices. What happens when the tool presents little to nothing of what is expected? What to do when the targeted app seems to not exist as far as the tool is concerned?

A big part of digital forensics involves what I call The Artisanal Approach. The Oxford Languages dictionary defines artisanal as:

ar·ti·san·al
/ärˈtēzən(ə)l/
adjective
- relating to or characteristic of an artisan.
“artisanal skills”
- (of a product, especially food or drink) made in a traditional or

[16] https://linqapp.com/abrignoni

non-mechanized way.
“artisanal cheeses”

This is just a long way of saying that we will rely have to manually identify the relevant data stores. The approach has 3 steps.

1. Locate the relevant apps.
2. Identify the data stores for the app and extract meaningful items.
3. Report generation.

On this chapter we will focus mostly on step number two. We will discuss what type of data stores are mostly seen in mobile forensics and suggest cost effective (i.e. cheap) solutions to traige these sources. Let’s dive in.

Locate Relevant Apps

The mobile forensics world is divided, mainly, between two dominant operating systems. These are Google’s Android and Apple’s iOS operating systems. As such both will organize things in vastly different ways within their file systems. This chapter will present examples from a full file system extraction view of Android and iOS devices. Even when working from a different type of extraction the main concepts, and the handling of data stores, will be the same. For details on mobile extraction types and their differences see here: https://privacyinternational.org/long-read/3256/technical-look-phone-extraction[17]

Is is important to note that this chapter will touch on the most common locations and types of data needed for analysis. It is not an all encompasing guide to mobile forensics nor does it intend to be so. Without further ado let’s dive in.

[17]https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

Relevant Apps in Android

In Adroid devices the apps keep most user generated data in the following directory:

/data/data/

As seen in figure 1 there are folders within the data directory for each app on the device. These folders are named in reverse URL format and are known as bundle identifiers (IDs.) For details on bundle IDs in Android see here: https://developer.android.com/studio/build/configure-app-module [18]

<img width="365" alt="figure 1" src="https://user-images.githubusercontent.com/28718987/162046213-9f7cce84-767b-4f81-bf0d-82e188f6a0f5.png">

Most mobile apps have bundle ID names that are easy to identify. Notice in the previous image how it is pretty obvious that com.android.chrome should be the bundle ID for the Chrome Browser, which it is. Another example would be how the bundle ID for Discord is com.Discord. Be aware that is not always the case. Not all bundle ID names are easy to reference back to the app name just by reading. One way of determining the budle ID of an app in Android is to look for the app in the Google Play store using a browser.

<img width="913" alt="Screen Shot 2022-04-06 at 2 23 04 PM" src="https://user-images.githubusercontent.com/28718987/162047421-6cf00abc-b101-4a60-b9e7-58cf4c38fefb.png">

The bundle ID is located in the URL at the top of the page.

https://play.google.com/store/apps/details?id=com.discord&hl=en_US&gl=US

[18] https://developer.android.com/studio/build/configure-app-module

Let's look at TikTok.

<img width="920" alt="Screen Shot 2022-04-06 at 2 21 53 PM" src="https://user-images.githubusercontent.com/28718987/162047835-30915faa-49be-424e-a8c4-e54a7f15ee23.png">

Notice how the bundle ID for TikTok, com.zhiliaoapp.musically makes no obvious reference to TikTok at all.

https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically&hl=en_US&gl=US

By changing the Google Play store URLs to the possibly unknown bundle IDs found on the target extraction one can determine the common app name for it.

Chapter 3

text goes here

Chapter 1