

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 2022-05-05



Leanpub

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.

© 2022 Andrew Rathbun, ApexPredator and Kevin Pagano

Contents

- Chapter 0 - Introduction 1
- Authors 2
- Chapter 1 - History of the Digital Forensics Discord Server 3
 - History of the Digital Forensics Discord Server 4
- Chapter 2 - Most Common Data Stores in Mobile Forensics 13
 - The Artisanal Approach 13
 - Locate Relevant Apps 14
- Chapter 3 - Chapter Title Goes Here 17
 - Subheading goes here 17
- Chapter 4 - I Have a Password Hash, Now What? 18
 - Disclaimer / Overview 18
 - The Basics 19
- Chapter 5 - Chapter Title Goes Here 20
 - Subheading goes here 20
- Chapter 6 - Chapter Title Goes Here 21
 - Subheading goes here 21
- Chapter 7 - Chapter Title Goes Here 22
 - Subheading goes here 22

CONTENTS

Chapter 8 - Chapter Title Goes Here	23
Subheading goes here	23
Chapter Nine	24
Chapter Nine - Gamification of DFIR: Playing CTF's . . .	25
What is a CTF?	25
Why am I qualified to talk about CTFs?	25
Types of CTFs	26
Evidence Aplenty	27
Who's Hosting?	28
Why Play a CTF?	29
Toss a Coin in the Tip Jar	31
Takeaways	36
Chapter 10 - Getting into Digital Forensics	37
So you want to be a digital forensic investigator?	39
Programming	39
Cooperation and Collaboration	39
International Cooperation	39
Chapter 11 - Chapter Title Goes Here	40
Setting Up a Law Enforcement Digital Forensics Laboratory 41	
Executive Cooperation	43
Physical Requirements	43
Selecting Tools	43
Certification and Training	43
Accreditation, Policy, and Procedure	43
Chapter 12 - Chapter Title Goes Here	44
Subheading goes here	44
Chapter 13 - Chapter Title Goes Here	45
Subheading goes here	45
Chapter 14 - Chapter Title Goes Here	46

CONTENTS

Subheading goes here	46
Chapter 15 - Chapter Title Goes Here	47
Subheading goes here	47
Chapter 16 - Artifacts as Evidence	48
Types of Artifacts	48
What is Parsing?	49
Artifact-Evidence Relation	50
Examples	51
Markdown Example	52
Section One	52
Including a Chapter in the Sample Book	52
Links	53
Images	53
Lists	54
Code Samples	55
Tables	56
Math	56
How Book.txt Works	57
Creating a Preview of Your Book	58
Getting Help	58

Chapter 0 - Introduction

TODO for Andrew

Authors

Author bios go here

Chapter 1 - History of the Digital Forensics Discord Server



DigitalForensicsDiscordServerLogoByKevinPagano

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 IRC¹ network called [freenode](#)². The channel was called #mobileforensics. This channel had its humble beginnings on a Google Group ran by Bob Elder of [TeelTech](#)³, called the [Physical and RAW Mobile Forensics Group](#)⁴, 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 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

¹https://en.wikipedia.org/wiki/Internet_Relay_Chat

²<https://en.wikipedia.org/wiki/Freenode>

³<https://www.teeltech.com/>

⁴<https://groups.google.com/g/physical-mobile-forensics/about?pli=1>

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 \(AIM\)](#)⁵ and [MSN Messenger](#)⁶ 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](#)⁷ 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 we were encountering during the acquisition or decoding process of a mobile device.

⁵[https://en.wikipedia.org/wiki/AIM_\(software\)](https://en.wikipedia.org/wiki/AIM_(software))

⁶https://en.wikipedia.org/wiki/Windows_Live_Messenger

⁷<https://hexchat.github.io/>

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](https://www.worldatlas.com/articles/how-many-countries-are-in-the-world.html)⁸ recognized in the

⁸<https://www.worldatlas.com/articles/how-many-countries-are-in-the-world.html>

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](https://support.discord.com/hc/en-us/articles/216273938-How-do-I-transfer-server-ownership)⁹ so that the server can live on without any administrative hiccups.

⁹<https://support.discord.com/hc/en-us/articles/216273938-How-do-I-transfer-server-ownership>

Chapter 2 - Most Common Data Stores in Mobile Forensics

By Alexis Brignoni

Online presence: <https://linqapp.com/abrignoni>¹⁰

The Artisanal Approach

Most mobile forensic examinations involve the use of third party tools to extract and decode information stored within 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

/är'tēzən(ə)l/

adjective

- relating to or characteristic of an artisan.

“artisanal skills”

- (of a product, especially food or drink) made in a traditional or

¹⁰<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>¹¹

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 encompassing guide to mobile forensics nor does it intend to be so. Without further ado let’s dive in.

¹¹<https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

Relevant Apps in Android

In Android 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>¹²

```

```

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 bundle ID of an app in Android is to look for the app in the Google Play store using a browser.

```

```

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>

¹²<https://developer.android.com/studio/build/configure-app-module>

Let's look at TikTok.

```

```

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 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 4 - I Have a Password Hash, Now What?

By John Haynes

YouTube - <https://www.youtube.com/channel/UCJVXolxwB4x3EsBAzSACCTg>

Disclaimer / Overview

This chapter will discuss some techniques and walkthroughs surrounding the cracking of password hashes. We will start with the basics and move into more advanced concepts and tools. The first and most obvious reason to know how to crack a password is to gain access to data that one has the legal right to access, but otherwise does not know the password. That being said, I do not condone, encourage, or support those who would use this information for malicious or illegal means. This brings us to the second reason for knowing how to crack a password, better security and protection against password cracking attempts.

For those that need to legally access the data, there should be something in here for you. For those that wish to learn how to better secure their own data, there should be something in here for you as well. That being said, let's get started!

The Basics

Chapter 5 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 6 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 7 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 8 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter Nine

Chapter Nine - Gamification of DFIR: Playing CTF's

By [Kevin Pagano](#)¹³ | [Stark 4N6](#)¹⁴

What is a CTF?

The origins of CTF or “Capture The Flag” were found on the playground. It was (still is?) an outdoor game where teams had to run into the other teams zones and physically capture a flag (typically a handkerchief) and return it back to their own base without getting tagged by the opposing team. In the information security realm it has come to mean a slightly different competition.

Why am I qualified to talk about CTFs?

Humble brag time. I’ve played in dozens of CTF competitions and have done pretty well for myself. I am the proud recipient of 3 DFIR Lethal Forensicator coins from SANS, one Tournament of Champions coin (and trophy!), a 3-time winner of Magnet Forensics CTF

¹³<https://twitter.com/KevinPagano3>

¹⁴<https://startme.stark4n6.com>

competitions, a 4-time winner of the BloomCON CTF competition, and a few others. I've also assisted in the creation of questions for some CTF competitions as well as creating thorough analysis write-ups of events I've competed in on [my personal blog](#)¹⁵.

Types of CTFs

Two of the most common information security types of CTF competitions are “Jeopardy” style and “Attack and Defense” style.

“Jeopardy” style typically is a list of questions with varying difficulty and set defined answers. The player or team is given some sort of file or evidence to analyze and then has to find the flag to the question and input it in the proper format to get points.

CHALLENGES

Binary	Forensics	Network	Pwnables	Web
BIN100	FOR100	NET100	PWN100	WEB100
BIN200	FOR200	NET200	PWN200	WEB200
BIN300	FOR300	NET300	PWN300	WEB300

Figure 1: Jeopardy style CTF

“Attack and Defense” is more common in Red and Blue team environments where the Red team has to hack or attack a Blue team server. The Blue team subsequently has to try and protect themselves from the attack. Points can be given for time held or for acquiring specific files from their adversary.

¹⁵<https://ctf.stark4n6.com>

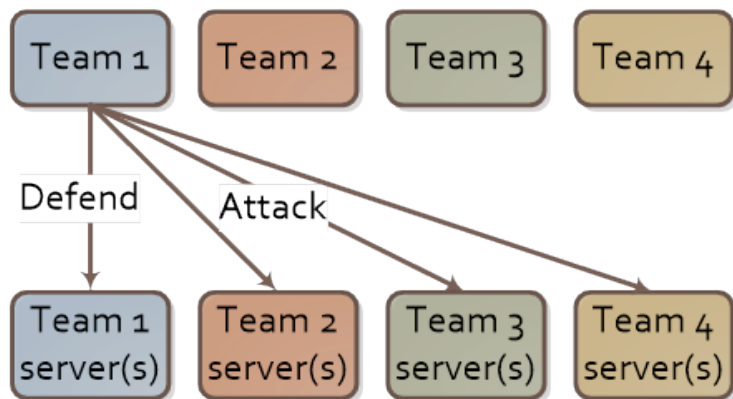


Figure 2: Attack and Defense CTF

Depending on the CTF, you may see a combination of types with it being Jeopardy style and linear (story based) with some questions hidden or locked until a certain question is answered.

For this chapter, I will go more in-depth regarding the “Jeopardy” style competitions, more specifically, forensics geared CTF competitions.

Evidence Aplenty

With forensics CTF's, just like in real life, any type of device is game for being analyzed. In the ever growing landscape of data locations, it just provides us more places to look for clues to solve the problems. One of the more well known forensic CTF's is the [SANS NetWars¹⁶](https://www.sans.org/cyber-ranges/) tournaments. These are devised with 5 levels with each level being progressively harder than the last. In this competition you will have a chance to analysis evidence from:

- Windows computer
- macOS computer

¹⁶<https://www.sans.org/cyber-ranges/>

- Memory/RAM dump
- iOS dump
- Android dump
- Network (PCAP/Netflow/Snort logs)
- Malware samples

You can see from the above list that you get a well rounded variety of types of evidence that you most likely will see in the field on the job. In other competitions I've played you could also come across Chromebooks or even Google Takeout and other cloud resources as they become more common. I have also seen some where they are more crypto based so working with different ciphers and hashes to determine the answers.

Who's Hosting?

As previously mentioned, SANS is probably the most well known provider of a forensics CTF through their NetWars program. It isn't cheap as a standalone, but is sometimes bundled with one of their training courses. You can sometimes see them hosted for free with other events such as OpenText's enFuse conference.

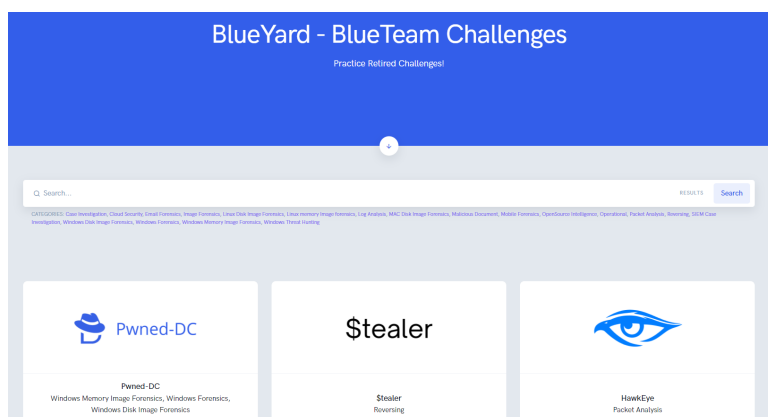
As for others, **Magnet Forensics** has been hosting a CTF for the past 5 years in tandem with their user summit. This has been created by Jessica Hyde in collaboration with some students from Champlain College's Digital Forensics Association. Some previous Magnet CTF's were also created by Dave Cowen and Matthew Seyer for context.

Other software vendors have started to create their own as well to engage with the community. **Cellebrite** in the past 2 years has hosted virtual CTF competitions and **Belkasoft** has created and put out multiple CTFs the last 2 years. **DFRWS**¹⁷ hosts a yearly forensic challenge with past events covering evidence types such as

¹⁷<https://dfrws.org/forensic-challenges/>

Playstation 3 dumps, IoT (Internet of Things) acquisitions, mobile malware, and many others.

Another fantastic resource for finding other challenges is **CyberDefenders**¹⁸. They host hundreds of various different CTF challenges, from past events and other ones that people have uploaded. You can even contribute your own if you'd like as well as allow them to host your next live event.



enter image description here

Figure 3: CyberDefenders website

Another fairly exhaustive list of other past challenges and evidence can be found hosted on **AboutDFIR**¹⁹.

Why Play a CTF?

So at the end of the day, why should YOU (yes, YOU, the reader) play a CTF? Well, it depends on what you want to get out of it.

¹⁸<https://cyberdefenders.org/blueteam-ctf-challenges/>

¹⁹<https://aboutdfir.com/education/challenges-ctfs/>

For Sport

Growing up I've always been a competitive person, especially playing sports like baseball and basketball, CTF's are no different. There is a rush of excitement (at least for me) competing against other like-minded practitioners or analysts to see how you stack up. You can even be anonymous while playing. Part of the fun is coming up with a creative handle / username to compete with. It also keeps the commentary and your competitors on their toes.

I personally like to problem solve and to be challenged which is part of the reason why I enjoy playing.

For Profit

I put profit in quotations because many may construe that as a compensation type objective. While many CTF challenges do have prizes such as challenge coins or swag (awesome branded clothing anyone?!) that's not completely the profit I'm talking about here. The profit is the knowledge you gain from playing. I've done competitions where I never knew how to analyze memory dumps at all and I learned at least the basics of where to look for evidence and new techniques to try later on in real world scenarios.

“Commit yourself to lifelong learning. The most valuable asset you'll ever have is your mind and what you put into it.” -
Albert Einstein

The knowledge you gain from the “practice” will inevitably help you in the future, it's just a matter of time. Seriously, you don't know what you don't know. Remember when I said you can be anonymous? It doesn't matter if you get 10 points or 1000 points, as long as you learn something new and have fun while doing so, that's all that matters.

Toss a Coin in the Tip Jar

I get asked all the time, “what are your keys to success playing CTFs?”. That’s probably a loaded question because there are many factors that can lead to good results. Here I will break down into sections that I feel can at least get you started on a path forward to winning your first CTF.

Tips for Playing - Prior

First and foremost is the preparation phase. Like any task in life, it always helps to be prepared for the battle ahead. Having a sense of what is to come will help with your plan of attack. Do your research! If you know that a specific person created the CTF then take a look at their social media profiles. Often times they will release hints in some form or fashion, whether it is webinars they have shared or research papers or blog posts they have recently published. Don’t over do it though, there could be red herrings amuck. You can also look at past CTF’s they have created, seeing how questions were formulated before and what sort of locations they tend to lean on for flags. This is part of the reason why I personally do write-ups of past CTF’s for future reference.

Each CTF rules may be different but if teams are allowed reach out to colleagues or others to form a squad. Knowledge from multiple people well-versed in different topics can help in spreading out the workload especially if there are multiple forms of evidence to be analyzed. I would be remiss if I didn’t say that some of my winning efforts were with team members who helped pick up sections where I wasn’t as strong. Your mileage may vary though, make sure to coordinate your efforts if you do join a team as to not waste time all working on the same questions.

If evidence is provided ahead of the competition make sure to spend some time getting familiar with it. Process the evidence ahead of

time so you aren't wasting time during the live competition waiting on machine time. Some of these events only last 2-3 hours so time is of the essence. This segues right into building out your analysis machine and your toolkit. Make sure that all your system updates are completed prior. The last thing you need is an errant Windows update to take down your system while you watch the spinning.

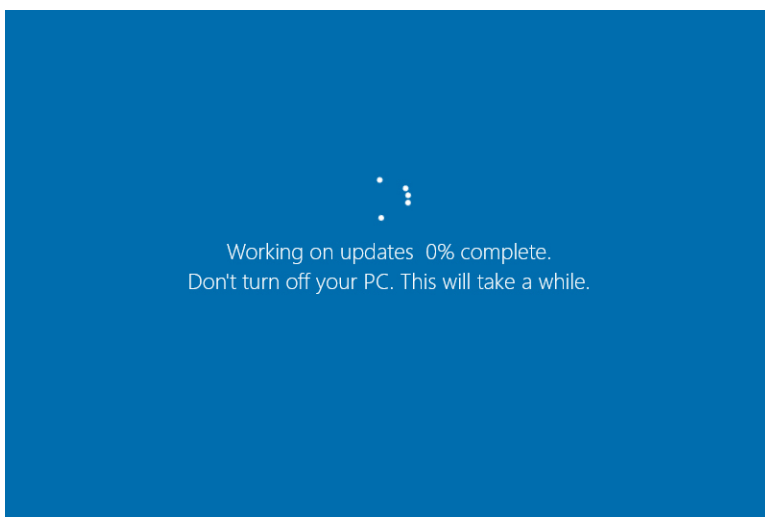


Figure 3: “This will take a while”

You may also consider making sure you have local admin access or at least the ability to turn off antivirus (if you are analyzing malware) to your computer. Always do so in a controlled environment if possible but you knew this already (I hope). If you are provided a toolkit or a trial of a commercial license, use it to your advantage, even if it's a secondary set of tools. There are times some vendors will make sure that the answer is formulated in a way that their tool will spit out from their own software. Also, commercial tools can potentially speed up your analysis compared to a bunch of free tools but that is personal preference.

The Toolkit

I'm a Windows user through and through so I cannot offer much advise from a Mac or Linux perspective. With that said, I do have some tools that I use from a forensic perspective to analyze those types of evidence. Here are my favorite (free) tools that I use during CTF's:

General Analysis

- Autopsy²⁰
- Bulk Extractor²¹
- DB Browser for SQLite²²
- FTK Imager²³
- Hindsight²⁴

Chromebook

- cLEAPP²⁵

Ciphers

- CyberChef²⁶
- dcode.fr²⁷

Google Takeout / Returns

- RLEAPP²⁸

Mac

- mac_ap²⁹
- plist Editor - iCopyBot³⁰

²⁰<https://www.autopsy.com/>

²¹https://github.com/simsong/bulk_extractor

²²<https://sqlitebrowser.org/dl/>

²³[https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,\(FTK%C2%AE\)%20is%20warranted.](https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,(FTK%C2%AE)%20is%20warranted.)

²⁴<https://dfir.blog/hindsight/>

²⁵<https://github.com/markmckinnon/cLeapp>

²⁶<https://gchq.github.io/CyberChef/>

²⁷<https://www.dcode.fr/en>

²⁸<https://github.com/abrignoni/RLEAPP>

²⁹https://github.com/ydkhatri/mac_ap

³⁰<http://www.icopybot.com/plist-editor.htm>

Malware/PE

- PESTudio³¹
- PPEE (puppy)³²

Memory/RAM

- MemProcFS³³
- Volatility³⁴

Mobile Devices

- ALEAPP³⁵
- Andriller³⁶
- APOLLO³⁷
- ArtEx³⁸
- iBackupBot³⁹
- iLEAPP⁴⁰

Network

- NetworkMiner⁴¹
- Wireshark⁴²

Windows Analysis

- Eric Zimmerman tools / KAPE⁴³
- USB Detective⁴⁴

This whole list could be expanded way further but this is the majority of the go-to's in my toolkit.

³¹<https://www.winitor.com/>

³²<https://www.mzrst.com/>

³³<https://github.com/ufrisk/MemProcFS>

³⁴<https://www.volatilityfoundation.org/releases>

³⁵<https://github.com/abrignoni/ALEAPP>

³⁶<https://github.com/den4uk/andriller>

³⁷<https://github.com/mac4n6/APOLLO>

³⁸<https://www.doubleblak.com/software.php?id=8>

³⁹<http://www.icopybot.com/itunes-backup-manager.htm>

⁴⁰<https://github.com/abrignoni/iLEAPP>

⁴¹<https://www.netresec.com/?page=NetworkMiner>

⁴²<https://www.wireshark.org/>

⁴³<https://ericzimmerman.github.io/#!index.md>

⁴⁴<https://usbdetective.com/>

Tips for Playing - During

We've all been there, you get to a point in the middle of a CTF and you start to struggle. Here are some things to key in on while actually playing.

Read the titles of the questions carefully, often times they are riddled with hints about where to look. "*Fetch*" the run time of XXX application, maybe you should analyze those Prefetch files over there. Questions will often also tell you what format the answer should be in when submitting. This may tell you that that timestamp you're hunting could be incorrect, those pesky timezone offsets!

Did you find a flag that appears to be a password? It's almost guaranteed that that evidence was placed in such a way that it will be reused. Emails and notes can be a treasure trove for passwords to encrypted containers or files.

One thing that may seem silly but can help is to just ask questions. If you're stumped on a question, talk to the organizer if you can, they may lead you in a direction that you didn't think of when you set off on a path of destruction.

Some CTF competitions have a built in hint system. If they don't count against your overall score, take them! The chances of a tie breaker coming down to who used less hints is extremely small. If the hint system costs points you will need to weigh the pros and cons of not completing a certain high point question as opposed to losing 5 points for buying that hint.

The last tip while playing is to write down your submissions, both the correct and incorrect ones. I can't tell you the amount of times I've entered the same answer wrongly into a question to eventually get points docked off my total. This will not only help you during the live CTF but afterwards if you are writing a blog on your walkthroughs.

Strategies

Takeaways

Chapter 10 - Getting into Digital Forensics



DFIRScience Logo

By Joshua I. James [DFIR Science](https://dfir.science)⁴⁵

v220405

⁴⁵<https://dfir.science>

So you want to be a digital forensic investigator?

Technical Skills

How to build a home lab?

Non-Technical Skills

WRITING

PRESENTING

Common Career Paths

Programming

Languages

Tools

Cooperation and Collaboration

Why Collaborate?

How to Collaborate?

Research

Conferences

Online Resources

International Cooperation

Informal

Formal

Chapter 11 - Chapter Title Goes Here

Setting Up a Law Enforcement Digital Forensics Laboratory

by Jason Wilkins MCFE, 3CE

Jason Wilkins Twitter“Follow Me on Twitter!”)

Executive Cooperation

The necessity of executive cooperation
Making your case to executive leadership
Open communication and trust

Physical Requirements

Physical security and accessibility
Floor plans

Selecting Tools

Network Requirements
Selecting forensic workstations
Selecting forensic software
Selecting peripheral equipment
Planning for Disaster

Certification and Training

Why should you get certified?
Where to find training
Creating a training plan for your lab

Accreditation, Policy, and Procedure

Accreditation requirements

Chapter 12 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 13 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 14 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 15 - Chapter Title Goes Here

Subheading goes here

Content goes here. Remember, only what is put here is parsed by Leanpub to generate the PDF/MOBI/EPUB files.

Chapter 16 - Artifacts as Evidence

Types of Artifacts

Digital Forensics is a six phase process including Preparation, Identification, Collection, Preservation, Analysis and Reporting.

Analysis is a major phase where in forensicators discover different types of artifacts ranging from plain metadata to complex evidence of execution and residual traces. The vast gap between the difficulty to retrieve or reconstruct evidence determines the fine line between E-discovery and Digital Forensics.

User data such as internet history, images, videos, emails, messages etc fall under E-discovery. It is relatively easy to reconstruct even from the unallocated space.

However, System Data like artifacts that help support some view of truth, or determine how closely a transpired event is to the evidence, are not that simple to manually parse with forensic soundness, which is why oftentimes forensicators rely on well-known parsing tools either commercial or opensource.



E-Discovery & Digital Forensics

And that is the main difference between E-Discovery & Digital Forensics depending on the categorization of data alone. Both follow different procedures and have different scope of execution. Generally, E-Discovery can be contained to only the logical partitions and the unallocated region whereas Digital Forensics operates

in a much wider scope solely due to the necessity of dealing with complex data structures.

What is Parsing?

Which brings us to parsing. We often go around throwing the term while working with a variety of artifacts; “Parse this, parse that”, but what does it mean in the real sense? To understand the parsing methodology, tools & techniques, we must be familiar with the origin of the handling of the data being parsed. What I mean by that is how was the data originally meant to be handled. What was it’s structure by design. How can it be replicated.

Generally, it is some feature or underlying mechanism of the main operating system installed on the device. Parsing tools are written to accurately mimic those functions of the operating system which make the raw data stored on the hardware, human readable.



Computer Structure

Understand the operating system as an abstraction level between the end-user and the intricacies of raw data. It provides an interface to the user which hides all the complexities of computer data and how it is being presented.

Artifact-Evidence Relation

You will come across an ocean of different artifacts in your investigations, but artifacts have a very strange relationship with what might potentially be considered evidence. Artifacts alone do not give you the absolute truth of an event. They provide you tiny peepholes through which you can reconstruct and observe a part of the truth. In fact, one can never be sure if what they have is indeed the truth in its entirety.



I always love to draw an analogy between the artifacts and the pieces of a puzzle, of which you're not certain to have the edge or the corner pieces. You gather what you can collect, and try to paint the picture as unbiased and complete as possible.



That being said, if you apply the additional knowledge from meta-data, OSINT and HUMINT to the parsed artifacts, you might have something to work with. For instance, say you were assigned an employee policy violation case, where the employee was using their work device for illegally torrenting movies. Parsing the artifacts alone will give you information around the crime, but not as evidence. You would still need to prove that the face behind the keyboard at the time of the crime, was indeed the one that your artifacts claim. So you would then look for CCTV camera footage around the premises, going back to the Identification phase in the digital forensics lifecycle, and so forth and so on.

As a result of a codependency of the artifacts on drawing correlations to some external factor, they form a direct non-equivalence relation with evidence.

However, note that this “rule”, if you will, is only applicable to a more broad scope of the investigation and will generally be handled by the lawyers. In the more narrow scope as a forensicator, and for the scope of your final forensic report, artifacts are most critical. Just keep it in the back of your mind that encountering an artifact alone does not mean it’s admissible evidence. Parse the artifact, make notes and document everything. Being forensically sound is more important than worrying about completing the entire puzzle. Because there will be no edge or corner pieces of the puzzle.

Examples

This section will cover how some of the more uncommon artifacts can play into a case from the bird’s eye view.

Registry

```
### Prefetch
### Shellbags
### Jumplists & LNK files
### SRUM
### $MFT
### $130
### $LogFile
### hiberfil.sys
```


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](https://leanpub.com/homepage)⁴⁶.

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:

⁴⁶<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](https://leanpub.com/markua/read#images)⁴⁷.

Lists

Numbered Lists

You make a numbered list like this:

1. kale
2. carrot
3. ginger

⁴⁷<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

```
1 puts "hello"
```

To learn more about adding code samples, see [this link](#)⁴⁸.

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](#)⁴⁹.

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.

⁴⁸<https://leanpub.com/markua/read#code>

⁴⁹<https://leanpub.com/markua/read#tables>

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

Something Involving Sums

To learn more about adding math, see [this link](#)⁵⁰.

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:

⁵⁰<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](https://leanpub.com/markua/read)⁵¹ 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.)

⁵¹<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!