I Care, But Where Do I Start? Sharing Knowledge in Digital Forensics

By
Josh Hickman (Kroll)

From the proceedings of
The Digital Forensic Research Conference
DFRWS 2020 USA
Virtual -- July 20-24

I Care, But Where Do I Start?

Sharing Knowledge in Digital Forensics

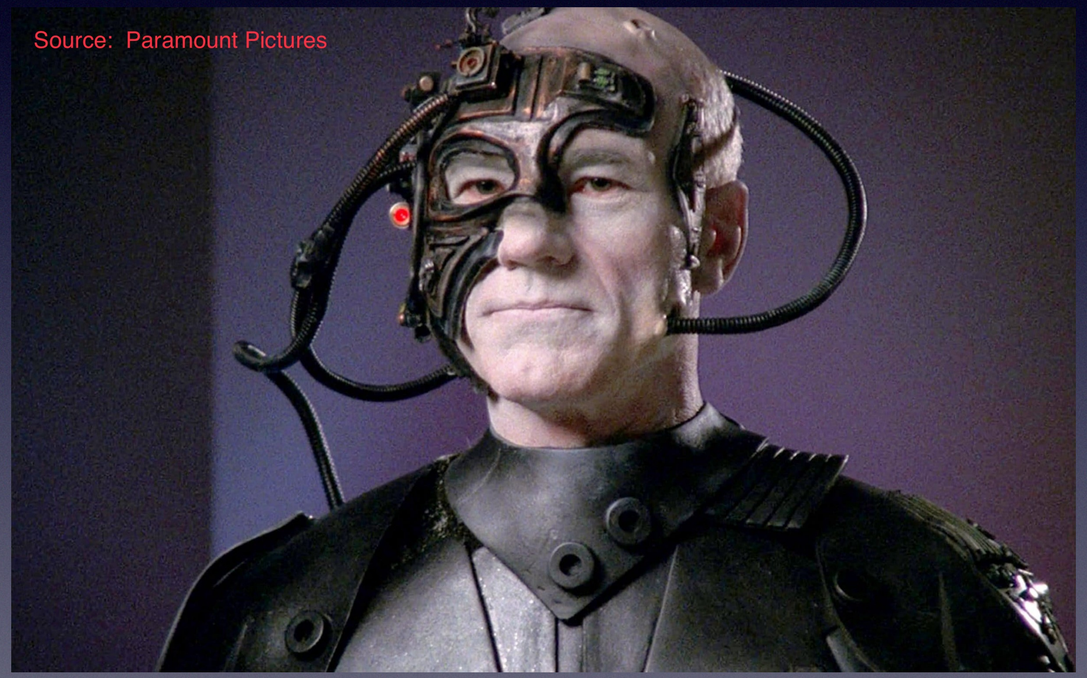
A Bit About Me…

Source: New Line Cinema

Common Obstacles to Sharing

Obstacle #1 - I Have Nothing to Say

- False
- If you conduct exams or research you have plenty to say
- Your experience can contribute to the DFIR body of knowledge.
- We are DFIR!



Obstacle #2 - What If I’m Wrong

AKA Imposter Syndrome

Ryuk and GPOs and Powershell, Oh My!

Binary Hick D… …ws December 22, 2019 11 Minutes

'Tis the season…for ransomware! Crooks, just like everyone else, are looking to make a little bit of extra money this holiday season so they can get their kids that GI J…e with the Kung-Fu grip (points for whoever gets the movie reference). Recently, I ha…n pushed to really pay attention to the Trojan/Ransomware lands…

Tweet

Josh Hickman
@josh_hickman1

Ryuk and GPOs and Powershell, Oh My!
#DFIR thebinaryhick.blog/2019/12/22/ryu…

21:32 · 12/31/19 · WordPress.com

View Tweet activity

Obstacle #3 - I Can’t Because...

- No Time
- Work Will Not Permit It - NDA, Criminal Investigation
- I don’t know how to blog

Tweet

Mattia Epifani
@mattiaep

Any idea of what's inside the PersonalizationPortrait folder on iOS? While developing the script I found a database named PPSQLDatabase.db. It seems really interesting (locations, contacts,..)
@HeatherMahalik @iamevltwin @AlexisBrignoni @B1N2H3X @forensicmike1 @josh_hickman1

06:35 · 6/2/20 · Twitter Web App

1 Retweet **15** Likes

Obstacle #3 - I Can’t Because...

- No Time
- Work Will Not Permit It - NDA, Criminal Investigation
- I don’t know how to blog

THIS WEEK IN 4N6

Your weekly roundup of Digital Forensics and Incident Response news

TIPS FOR STARTING A BLOG

I've had a few people ask for tips on blogging, and thought I'd put it all in one place. I also put down a few reasons why you should create your own home on the web here.

- Set a schedule. I post here on Sundays, at the end of every month, and at the end of every year. At least that's the goal.
  On ThinkDFIR, I aim to post once a month...when you think about that, that's only 12 posts a year. Some people are crazy and post every day, and that's a daunting and difficult task that many people have tried. Limiting to 12 posts + when inspiration strikes means that you can write out a few draft posts in advance and then you're already ahead!

- Not everything has to be groundbreaking. You can test your understanding of an artefact, you

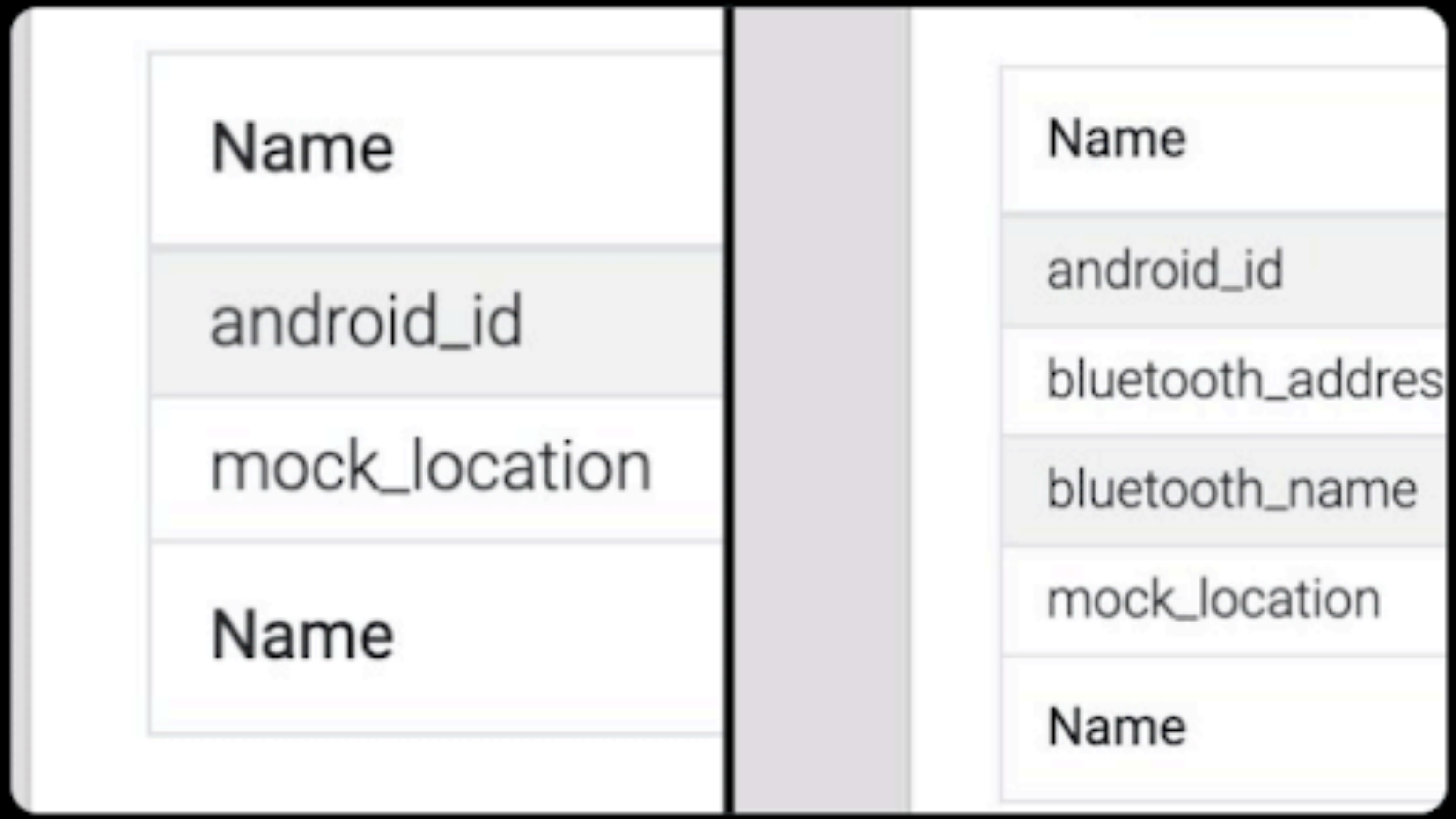
Ways To Share

Twitter

- Yes, Twitter.
- #DFIR
- Easy and quick way to share bits of knowledge without having to write very much.

Brigs @AlexisBrignoni · 4/2/20

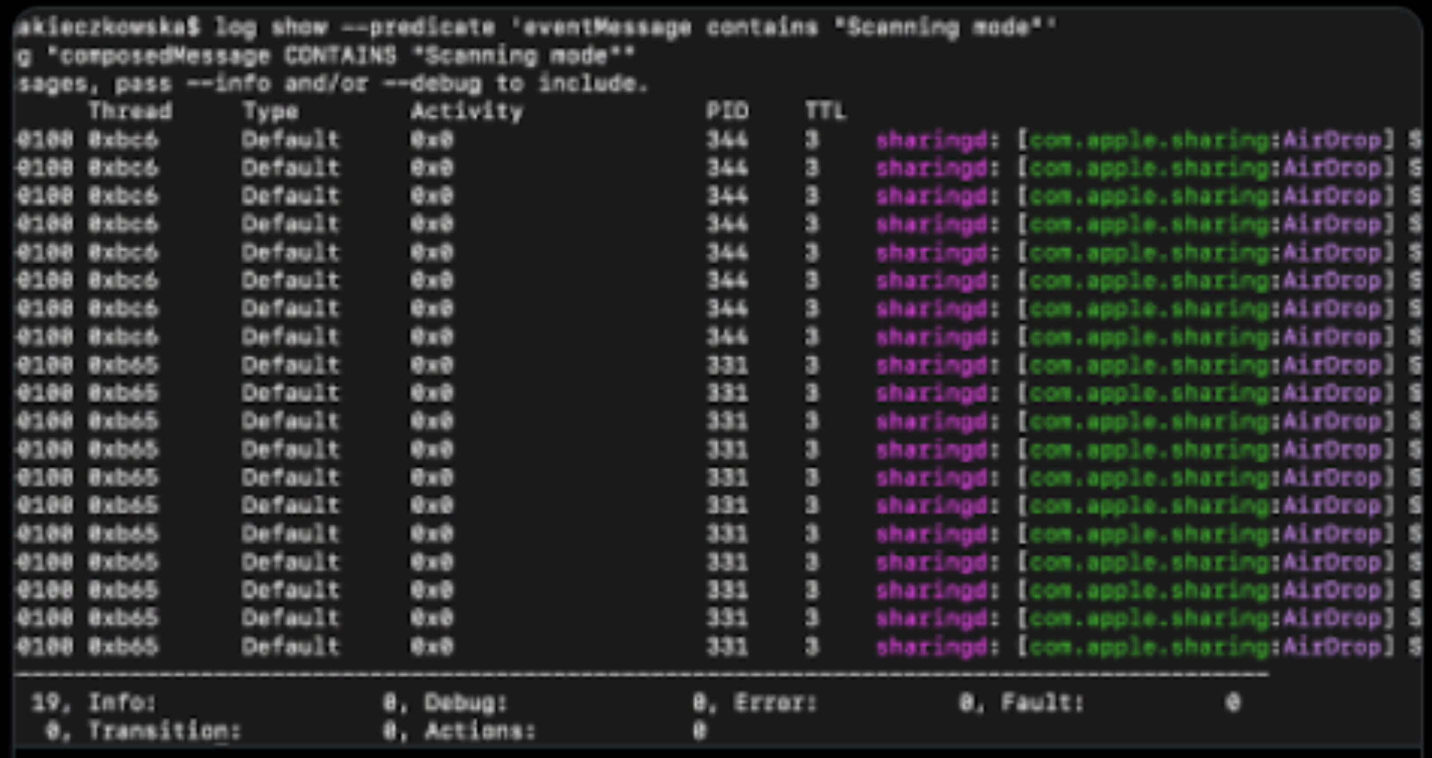
Just noticed that if you parse an Android phone that has more than one user you get two distinct securesettings.xml files with distinct Android_IDs per file/account. Not sure about #DFIR applicability of the IDs yet, just found it interesting.



1 · 2 · 11

Sarah Edwards @iamevltwin · 6/29/20

Great stuff! It brought me to your other AirDrop one, kieczkowska.com/2020/06/15/air.... I believe the reason you were not seeing the same results as my iOS example is that macOS likes to save those as Info messages. Try passing - -info to get those messages. 👍



AirDrop Forensics
kieczkowska.com

1 · 1 · 5

Josh Hickman
@josh_hickman1

#DFIR Of course Samsung would choose to use their own version of #Android Digital Wellbeing. Database sits in /data/data/com.samsung.android.forest. Name is dwbCommon.db. 1/3

```
com.samsung.android.calendar
com.samsung.android.cidmanager
com.samsung.android.clipboarduiservice
com.samsung.android.contacts
com.samsung.android.container
com.samsung.android.da.daagent
com.samsung.android.dialer
com.samsung.android.dqagent
com.samsung.android.drivelink.stub
com.samsung.android.dsms
com.samsung.android.dynamiclock
com.samsung.android.easysetup
com.samsung.android.emojiupdater
com.samsung.android.fmm
com.samsung.android.forest
com.samsung.android.game.gamehome
com.samsung.android.game.gametools
com.samsung.android.game.gos
com.samsung.android.incallui
com.samsung.android.ipsgeofence
com.samsung.android.kgclient
```

8:23 AM · 5/21/20 · Twitter for Mac

Ryan Benson @_RyanBenson · 7/2/20

#DailyDFIR 184: Have a number you suspect is a timestamp? Pass it to Unfurl! 🌿

It will convert if it's a "plausible" value (year 2015-2025) for any of these timestamp types:

- 🕓 Unix epoch micro/milli/centi/seconds
- 🕓 Webkit
- 🕓 Windows FileTime/DateTime
- 🕓 Mac/Cocoa

#DFIR

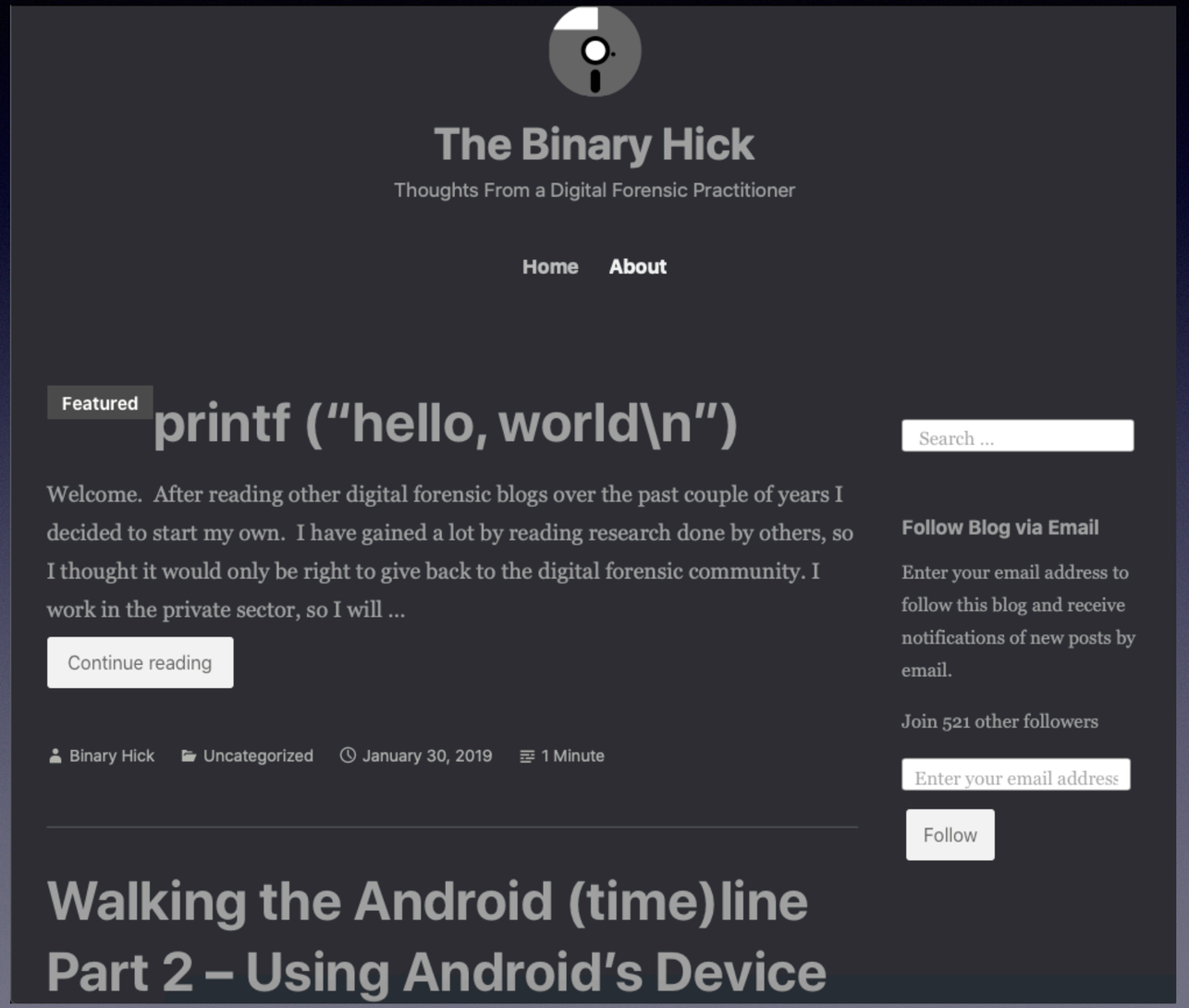
```
C:\Users\Ryan
λ unfurl_cli.py 1586398602054267
[1] 1586398602054267
 └─(🕓)─[2] 2020-04-09 02:16:42.054267

C:\Users\Ryan
λ unfurl_cli.py 1586398602054267 -d
[1] 1586398602054267 (type: url)
 └─(🕓)─[2] 2020-04-09 02:16:42.054267 (
microseconds) -- Converted as Epoch  mic
```

1 · 14 · 39

Blogging

- More involved (time, resources)
- Can share more detailed information



AboutDFIR.com – The Definitive Compendium Project
Digital Forensics & Incident Response

HOME | WHO WE ARE | SUBMIT | COMMUNITY | EDUCATION | JOBS | READING | RESEARCH | RESOURCES | TOOLS & ARTIFACTS

Contributors

Devon Ackerman is the digital forensicator and incident responder behind the DFIR Definitive Compendium Project. Currently employed as a Managing Director at Kroll Cyber Risk...

Read More ›

DFIR Research

The DFIR Research list is a list of potential digital forensic and incident response research projects contributed by community...

Read More ›

DFIR & Cybersecurity Careers

Looking to transition into the world of Digital Forensics, Incident Response, Cyber Security, etc? This page is for you. Employers will list opportunities...

Read More ›

Featured Page of the Month

July 2020's Featured Page of the Month is the Awards page! The Forensic 4:cast Awards will be announced July 17, 2020! Cast your votes before it's too late!

Read More ›

DFIR Training
Digital Forensics-Incident Response

HOME | TOOLS | TRAINING | ARTIFACTS | RESOURCES | DIRECTORIES | BOOKS | BLOG | SEARCH | CONTACT

What's New at DFIR Training

June 20, 2020. Regularly updated, never outdone, check out the latest additions to keep up on your DFIR training! Website updates. DFIR Subcontractor listings, Forensic Artifacts and more.

CHECK OUT "WHAT'S NEW AT DFIR TRAINING"

ABOUT | SUPPORT THE PROJECT | TIPS FOR STARTING A BLOG | PODCAST | RESOURCES | CONTACT

THIS WEEK IN 4N6

Your weekly roundup of Digital Forensics and Incident Response news

WRITTEN BY PHILL MOORE
JULY 12, 2020

Search ...

FOLLOW BLOG VIA EMAIL

WEEK 28 – 2020

Less than a week to go until the (Virtual) DFIR Summit! Our very own Lodrina is even keynoting on day 2!

Also not long till the Forensic 4Cast awards so get your votes in quick!

As always, thanks to those who give a little back for their support!

FORENSIC ANALYSIS

- Arman Gungor at Metaspike
  Gmail History Records in Forensic Email Investigations

DFIR DIVA | Digital Forensics and Incident Response Blog Geared Toward Beginners

Home | About Me | DFIR Resources | Blog Categories | Free Training | Getting Into the DFIR Field | Subscribe | COVID-19 Discount List

Hello and Welcome to my Blog!

Posted on February 14, 2020 by DFIR Diva Uncategorized

I entered the DFIR field in May of 2019 and created this site to document the resources I use as I learn and grow in DFIR. I'm hoping it will help others who are interested in the field or who are also just getting started. Under DFIR Resources, you will find books, training, webinars, videos, and other resources that I have found to be helpful. I also use Facebook and Twitter to share resources I come across. This is a personal blog and all views are my own.

Continue reading...

To search type and hit enter

DFIR Related Events for Beginners – July 2020

ZENA FORENSICS

something about digital forensics and something not

Checkra1n Era - Ep 6 - Quick triaging (aka from the iPhone to APOLLO, iLEAPP and sysdiagnose in 6 minutes)

By Mattia Epifani - June 05, 2020

Over the last months, a lot of research based on the **checkm8 exploit** was done.
On **data acquisition**:
Belkasoft, Cellebrite and MSAB developed a "forensic-oriented" implementation of th
exploitElcomsoft, Oxygen and Magnet Forensics support a full file system extraction

Post a Comment

BYOM - Build Your Own Methodology (in Mobile Forensics)

By Mattia Epifani - April 26, 2020

Last Friday I had the honour to present at "Life has no CTRL+ALT+DEL", a DFIR online meetup organized by Heather Mahalik in this crazy COVID-19 period.

mac4n6

Blog
Contact
Resources
Training & Events

Socially Distant but Still Interacting! New and Improved Updates to macOS/iOS CoreDuet interactionC.db APOLLO Modules

June 21, 2020 in iOS, APOLLO, macos, analysis

The interactionC.db database certainly does not get as much as attention as its CoreDuet partner in crime, knowledgeC.db. However, I think it has quite a bit of investigative potential. I've written about it before in a prior blog, however I'd like to give it more attention here.

I spent this weekend updating the APOLLO modules to have more contextual support and better backwards compatibility with older iOS versions. This database was also introduced to the macOS side with 10.15.

I've added a new query for this database for the ZKEYWORDS table. This tables appears to capture keywords that are contained in various Calendar (com.apple.mobilecal) events. It seems only select certain events as not all my calendar event has keywords in this table.

The main interactionsC.db query has many new updates including attachments and sender/recipient correlation. In general, this database is keeps track of "recent" contact interactions. As an example, I used this query on my iOS database that I copied off of my iPhone a few days ago and it shows ~28,00 entries going all the way back to January of this year, 6+ months!

In the screenshot below is a Messages (com.apple.MobileSMS) conversation between Heather I and I. Items that are blurred are our phone numbers. The GUIDs are our Contact Person IDs, the be correlated with Information in the iOS Address Book database. Why some recipient informati blank, I'm not sure. I scrolled way back in our conversation history and the timestamps are spot

Windows Incident Response

The Windows Incident Response Blog is dedicated to the myriad information surrounding and inherent to the topics of IR and digital analysis of Windows systems. This blog provides information in support of my books; "Windows Forensic Analysis" (1st thru 4th editions), "Windows Registry Forensics", as well as the book I co-authored with Cory Altheide, "Digital Forensics with Open Source Tools".

Tuesday, July 07, 2020

On Artifact Constellations And "Toolmarks"

Something I've been pretty focused on in my analysis for some time is the concept of "artifact constellations". I originally referred to this concept as "artifact clusters", but I heard someone from the FBI's Cyber BAU team use the term "constellations", and co-opted the term, in part to facilitate our conversation, but also because it sounded much more appropriate.

Artifact constellations are found as a result of events (not *an* event, but events) that occur on a system within close *temporal proximity* (another borrowed term, this one from Mr. Walters), as a result of some action, taken either by the user or threat actor. When someone interacts with the operating system and applications, there are direct artifacts as a result of that interaction. There are also very often indirect artifacts, created as a result of the events occurring within the "eco-system"; that is, events generated by the operating system but are not a result of direct interaction by the user.

Artifacts should never be viewed in isolation, as this can lead to incorrect findings when an artifact constellation is completed with assumption. This can be an issue, among other instances, when examining artifacts of program execution. For example, if an analyst were to find a prefetch file or a UserAssist entry for CCleaner, does this mean that the user executed the capabilities of CCleaner, or simply that they launched the GUI? When viewing only artifacts such as a prefetch file or a UserAssist entry in isolation, there is qualitatively no difference between launching CCleaner and taking advantage of its full capabilities, and simply launching the CCleaner UI, waiting a few minutes, and closing the application.

Artifact constellations will vary in the number of artifacts they contain, based on a number of factors, such as the version and configuration of the operating system, the version and

Pages
Home
Timelines
Books
Malware
FOSS Tools

Subscribe To WindowsIR
Posts
All Comments

WindowsIR Blog List
DFIR and Threat Hunting
Insider Threat Hunting
6 days ago
JPCERT/CCブログ 英語

James Duffy

Blog | Oxygen | Projects | Courses | About | Contact/Donate | My Blog

Jun 26 • Written By James Duffy

KnowledgeC.db - The iOS Database that knows more about you than you.

Gooooooood morning!

Today is my day off, following **61 good ol' days of research, articles and projects**. I couldn't help myself

Cheeky4N6Monkey

Smarter Forensics

It's time to get SMARTER!

Search ...

RECENT BLOG POSTS

"Life Has no ctrl+Alt+Del" – The New DFIR online Meetup
2020 Forensic 4Cast Nominations are open!
iOS 13 – Summary for those of you who enjoy the cliffsnotes
...Won't you back that thing up: a glimpse of ios 13 artifacts
I'm not hiding, I swear!

ARCHIVES

April 2020
March 2020
September 2019
January 2019
August 2018
June 2018
March 2018
October 2017
September 2017
August 2017
December 2016
September 2016
August 2016

ABOUT US | BLOG | CONTACT US | PAPERS, SCRIPTS AND MORE | PRESENTATION

ABOUT US

Smarter Forensics was initially developed by Heather Mahalik to share, post and promote all items pertaining to digital forensics. All items listed on this website are deemed helpful by Heather and are not solicited by companies and vendors (other than Smarter Forensics).

The Reading Room will contain white papers and links to articles by those in the community. Please let me know if you have something to contribute to the reading room.

Don't forget to check out the blog for interesting topics and conversations.

Open "https://smarterforensics.com/about-us/coin/" in a new tab

Initialization vectors

Digital Forensics and Incident Response. All things InfoSec.

Thursday, July 9, 2020

DFIR Resources

This blog post is a link repository for content created by me that is related to xLEAPP and Python for digital forensics.

Youtube channel:
https://www.youtube.com/channel/UCdss8CLyyNGgrXgzFaF9rNw

16 videos — DFIR Python Study Group — Basic Python course

4 videos — xLEAPP Usage & Artifact Development — Videos on how to use and develop artifacts in iLEAPP

Follow @AlexisB

Search This Blog

Blog Archive
2020 (12)
July (1)
DFIR Resources
June (1)
May (1)
April (2)
March (2)

HOME

HACKING EXPOSED

COMPUTER FORENSICS BLOG

BY DAVID COWEN

A Blog on computer and digital forensic research, DFIR programming, the forensic lunch and more wirrten by Hacking Exposed Computer Forensic author David Cowen

Latest News

Daily Blog | Daily Blog #685: Sunday Funday 4/26/20

Daily Blog | Daily Blog #684: Solution Saturday 4/25/20

DOUBLEBLAK DIGITALFORENSICS

Home | Blog | Links | Software | Group

"What one man can invent, another ca

Ian Whiffin

DoubleBlak Digital Forensics is a Digital Forensics website aimed at helping fo evidence.

It is maintained by a Ian Whiffin, a Law Enforcement Officer / Digital Forensics agency.

With over twenty years experience in IT, 15 years in Policing (split between Ca Digital Forensics, Ian has been qualified as a Subject Matter E experience in the examination of computers, cell phones and but has created software tools to fill the gaps left by vendors. Software section of this site (Requires authentication).

Ian is trained with numerous forensic software tools related to ChipOff, ISP, Visual NAND Reconstructor and enjoys tinkering his own software for many years using numerous different lan Javascript.

Yogesh Khatri's forensic blog

All things forensic and security related

Home | Downloads | About

SEARCH BLOG

Search

BLOG ARCHIVE
2020 (4)
June (1)
Screentime Notifications in Catalina (10.15)
March (2)
January (1)
2019 (4)
2018 (8)
2017 (7)
2016 (3)
2014 (3)
2013 (10)
2012 (8)
2011 (4)
2010 (1)

(10.15)

ably done a few macOS Catalina (10.15) examinations
ata, you may have noticed that for ScreenTime notifications
t you see in the actual displayed Notification and several

2 days ago

ble
47 minutes of screen time

ons database. For macOS High Sierra (10.) and above, it is

otificationcenter/db2/db

Another Forensics Blog

Digital Forensics and Incident Response Research,Python Scripts and Musings

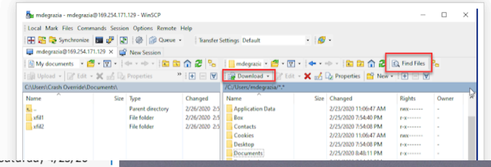
Home | Downloads | Mac Imaging

Thursday, February 27, 2020

Detecting Lateral Movement with WinSCP

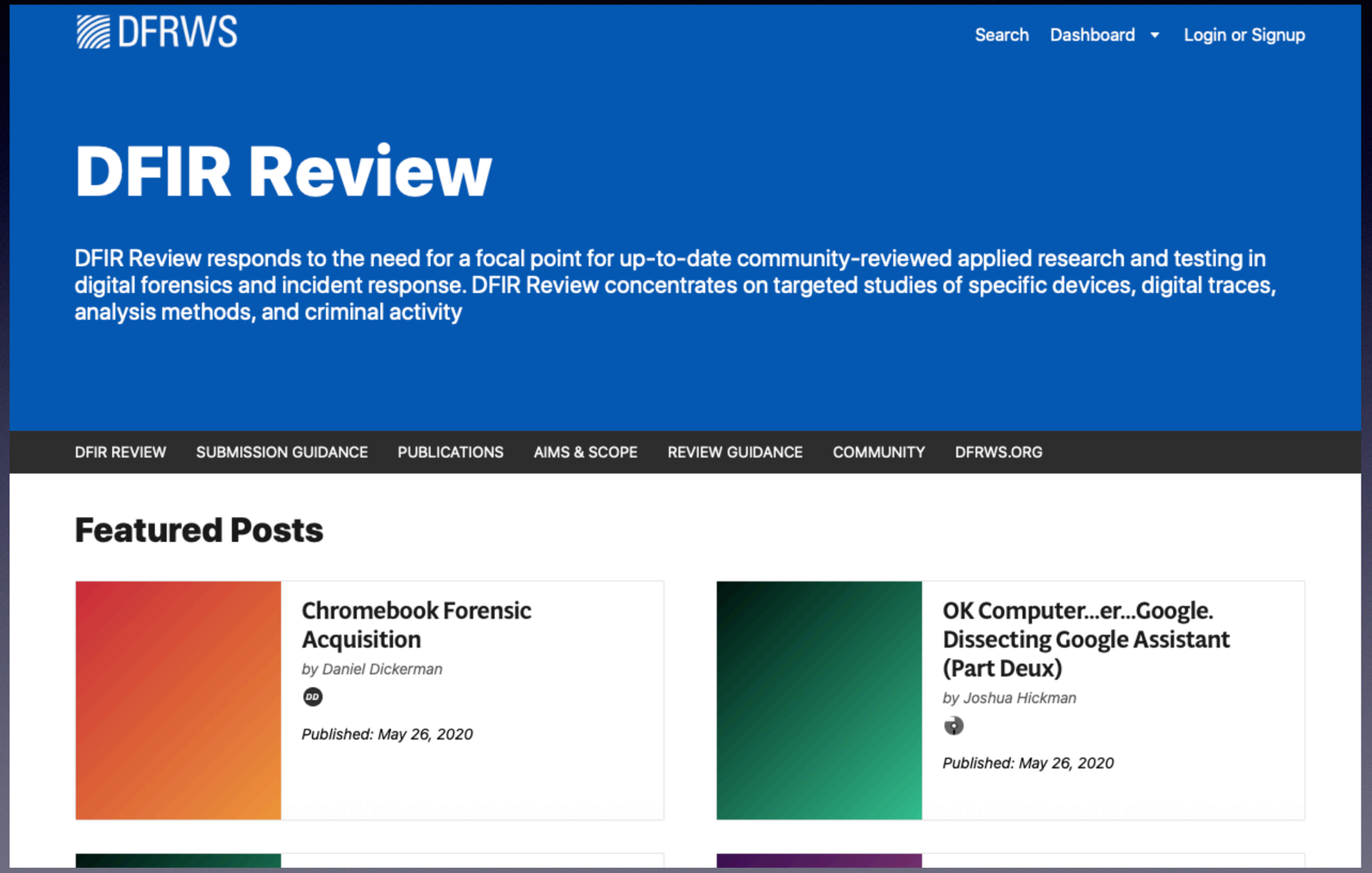
RDP is a common way for an attacker to move laterally within an environment. Forensically, when an attacker uses RDP we can use artifacts such as shellbags, link files and jumplists on the remote system to see what was accessed while the attacker was RDPed into the system.

Another way an attacker can access a system remotely is to use a program called WinSCP. Using WinSCP, they can browse folders and files on a remote system, copy folder and files back to the system they are currently on, and even search the remote system for files!



DFIR Review!

- DFRWS initiative
- Peer-review of blog posts
- DOI Number!



iOS Mobile Installation Logs

What applications were installed on an iOS device and when?

by Alexis Brignoni

CITE [#]
SOCIAL
DOWNLOAD
CONTENTS

last released
1 year ago

Synopsis

Forensic question: What applications were installed on an iOS device?

OS Version: iOS 11, iOS 12

File: /private/var/installd/Library/Logs/MobileInstallation/*.log

Tools: Python

Introduction

In the last two blog posts I wrote about ways of obtaining a list of currently installed apps and their corresponding app directories from an iOS file system extraction. My usual method is to query the contents of the applicationState.db file to find the app bundle id and what directory GUID

DFIR Review

This work details how to extract and interpret app installation logs from an iOS file system to determine which applications are currently installed and that were deleted. A comprehensive list of app installation activities, including timestamps, can be very useful in an investigation of a mobile device.

This work provides a Python script and a dataset for testing the script.

Using the test dataset provided by the author, in mobile_instalation.log.0 there were no results for System_State - Validated manually the log and the sql database created and this is correct. The mobile_installation.log.0 file from my personal test data did have entries. Both are correct parsing of the log. Manually reviewed data from provided mobile_instalation.log.1 to results in Apps_Historical, Apps_State, System_State, and the created mib.db for both test data from author and own test data. Both are correct. This script worked as expected on both the provided test data and data that I created.

Future Work

Installations with errors are not displayed in the database or in any of the text documents, there may be value in including those times in the Apps_Historical txt documents for the bundleID.

Reviewers

Questions?

Joshua Hickman

Twitter: @josh_hickman1
Blog: https://thebinaryhick.blog