



米国における DFコンテストの状況と 日本における展開の可能性

立命館大学情報理工学部

デジタル・フォレンジック研究会副会長

上原哲太郎

R 米国におけるDFコンテスト

- 米国の学会や集会ではTutorialが盛ん
- ただしそれなりに参加費を取る
- 有料開催される高額なTutorialに対し、参加費廉価 or 無料な競技は多くの場合 Capture the Flag (CTF)として開催
DFに特化したものは Forensic Challenge等の名前で開催される
(またはDFIR: Digital Forensics & Incident Response)
- 有名なものはDEFCON DFIR CTFや DFRWS Forensic Challenge等



典型的なForensic Challenge

- Forensicの対象となるデータが主催者側から提供される
 - ddなどのHDDイメージ
 - pcapなどのパケットキャプチャイメージ
 - その他ログや関連データ等
- その上で出されるクイズに答える
 - 侵入されたアカウントはどれか？いつか？等
- Tutorialの題材としても多用される



SANS DFIR Challenge

<https://digital-forensics.sans.org/community/challenges>

- 元々 LMG Security 社が何度か提供した Network Forensics Puzzle Contest から引用したもの
 - 2010年5月に提供された Puzzle #6: Ann's Aurora
 - Ann が "Secret Sauce recipe" を 標的型攻撃で盗み出したログを pcap から読み取ろうというチャレンジ

R Ann's Auroraで聞かれること

- 被害者が踏んだURL (URI)
 - その結果としてのJavaScriptの挙動
 - その結果としてリクエストされたファイルの名前とMD5ハッシュ
 - 結果として4444ポートが開いた時間
 - 4444ポートが閉じた時間
 - さらに送られたファイルについての情報
- Etc...

DFRWS Forensic Challenge



DFRWS Forensic Challenges are open to all participants and are designed to be accessible at multiple skill levels. Some answers will be accessible to participants with basic digital forensic skills, and more advanced elements are included. Examples of previous challenge submissions, including the grand prize winners, are available here.

DFRWS IoT Forensic Challenge (2018 - 2019)

Submission deadline: Mar. 20, 2019

Scenario:

On 17 May 2018 at 10:40, the police were alerted that an illegal drug lab was invaded and unsuccessfully set on fire. The police respond promptly, and a forensic team is on scene at 10:45, including a digital forensic specialist.

The owner the illegal drug lab, Jessie Pinkman, is nowhere to be found. Police interrogate two of Jessie Pinkman's known associates: D. Pandana and S. Varga. Pandana and Varga admit having access to the drug lab's WiFi network but deny any involvement in the raid. They also say that Jessie Pinkman's had the IoT security systems installed because he feared attacks from a rival gang and that Jessie kept the alarm engaged in "Home" mode whenever he was inside the drug lab.

Within the drug lab the digital forensic specialist observes some IoT devices, including an alarm system (iSmartAlarm), three cameras (QBee Camera, Nest Camera and Arlo Pro) as well as a smoke detector (Nest Protect). An Amazon Echo and a WinkHub are also present.



HACKING EXPOSED

COMPUTER FORENSICS BLOG

BY DAVID COWEN

Monday, August 13, 2018

Daily Blog #451: Defcon DFIR CTF 2018 Open to the Public

Hello Reader,

This year at Defcon we made things interesting with a challenge that involves making your way through 3 images to answer questions and solve a case. Now that Defcon is over and the winners awarded it's your turn to give the challenge a try.

The first image password is 'tacoproblems'

The second and third image password is gained by answering the right questions in the CTF.

CTF Site:

<https://defcon2018.ctfd.io/>

Download Links:

Image 1:

<https://www.dropbox.com/s/1q4f0fowo8048mq/image1.7z?dl=0>

Image 2:

<https://www.dropbox.com/s/9gzjfqki8uup58k/image2.7z?dl=0>

Image 3:

<https://www.dropbox.com/s/jvaqb4rfi3jojbk/image3.7z?dl=0>

7

Beyon

Posted by David Cowen at 3:13 PM

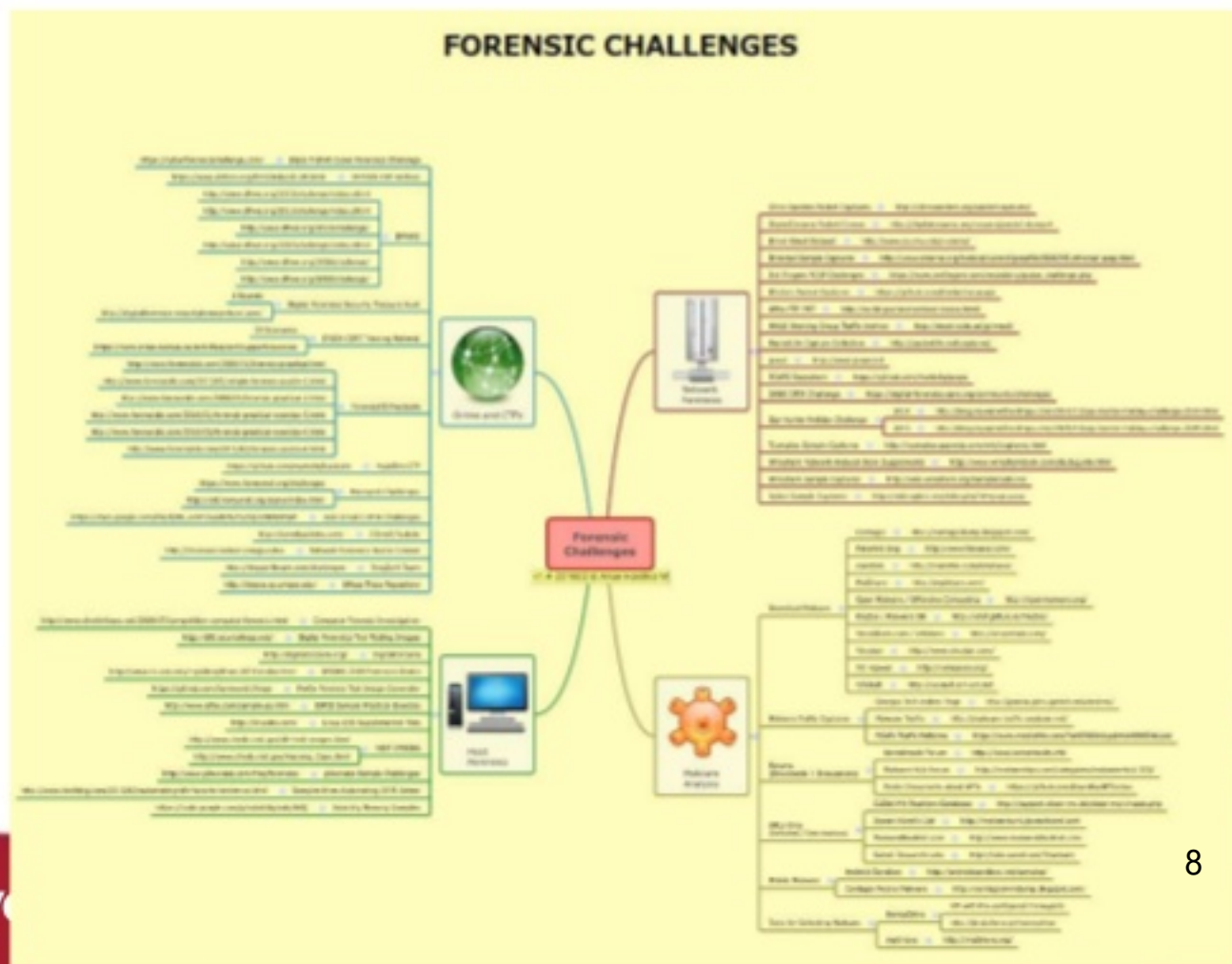


Lab <https://www.hecfblog.com/2018/08/daily-blog-451-defcon-dfir-ctf-2018.html>



Aman Hardikar氏による分類

<https://www.amanhardikar.com/mindmaps/ForensicChallenges.html>



R DFコンテストの効果？

DFコンテストの題材として
dd / pcapのimageと
QUIZが公開される

これを元にDF / IRの
練習をする人が増え
DF技術者が増える

挑戦した人が解き方と
自分が出した答えを
Blog等でWrite upをまとめる

正解も公開される等して
これらがネット上に
蓄積される

R Write upの例

Defcon DFIR CTF 2018 Writeup

By infosecuritygeek 目 Digital forensics 1 Comment

Hello everyone! This is my write-up for the Defcon DFIR CTF which was opened to the public last August 14, 2018 as announced by [David Cowen](#) on Twitter. This is probably my first time joining a CTF that is purely DFIR related and I must say that I really enjoyed doing an investigation style CTF (please keep em coming!). Luckily, I managed to finish all the challenges and place 4th overall.

Place	Team	Score
1	g0tmi1k	200
2	viviasix	200
3	nightal	200
4	uP13n	200
5	hackerhoney	200

Challenge Background

The challenge is comprised of several questions with varying difficulties (basic, advanced, and expert) in which you have to analyze three forensic images (HR Server, File Server, and Desktop) in order to get the correct answers. The images are zipped and password protected initially so the participants need to acquire certain points or answer certain questions in order to unlock the password for the next image.

7x Passwords:

- Image 1: tacoproblems
- Image 2: tacounities
- Image 3: viviaa(pastortacos)

Th <https://infosecuritygeek.com/defcon-dfir-ctf-2018/>


2018/11 Defcon DFIR CTF 2018 Writeup(HR Server + File Server)

22

モチベーションとか

今年の8月頃、Defcon DFIR CTF 2018 が一般公開されたという記事(This Week in 4n6)を見て、とりあえずイメージファイルだけ取ってそのまま忘れていた。

Week 33 - 2018
FORENSIC ANALYSIS Justin Benavente walks through a few of the site facts that are useful for tracking USB devices on a Windows system. I also described his recent internship at CalForensics DFS.




<https://www.4n6.com>

<https://www.4n6.com>

10月に大和セキュリティさんが開催した「DFIR初心者チャレンジ」に参加して、もっとForensicsの勉強をしたいという気持ちになり、このCTFのことを思い出ししたのでやってみた。暇を見つけつつのんびりやったので、最初の方と最後の方で使っている環境やツールが違ってたりするけど気にしないで欲しい。

DFIR初心者チャレンジは凄く勉強になりました。

TMCIT × 大和セキュリティ勉強会DFIR初心者チャレンジ (2018/10/7-8) (東京) (2018/10/07)
• 数ヶ月間の所属する株式会社PCに不正アクセスされた感があります。思い込んでHDDイメージ、メモリアンプ、ネットワークキャプチャデータがある。4月20日に神戸にて開催し



<https://www.tmcit.com>

<https://www.tmcit.com>

以下のページにCTFサイトのURLと、イメージファイルのダウンロードリンクが貼られている。

Daily Blog #451: Defcon DFIR CTF 2018 Open to the Public
A blog about computer and digital forensics and techniques, hacking exposed dfir incident response file systems journaling

10

<http://ecoha0630.hatenablog.com/entry/2018/11/22/180306>



The CFReDS Project

NISTがDF用の イメージを収集公開

NIST is developing **Computer Forensic Reference Data Sets (CFReDS)** for digital evidence. These reference data sets (CFReDS) provide to an investigator documented sets of simulated digital evidence for examination. Since CFReDS would have documented contents, such as target search strings seeded in known locations of CFReDS, investigators could compare the results of searches for the target strings with the known placement of the strings. Investigators could use CFReDS in several ways including validating the software tools used in their investigations, equipment check out, training investigators, and proficiency testing of investigators as part of laboratory accreditation. The CFReDS site is a repository of images. Some images are produced by NIST, often from the CFTT (tool testing) project, and some are contributed by other organizations. National Institute of Justice funded this work in part through an interagency agreement with the NIST Office of Law Enforcement Standards.

In addition to test images, the CFReDS site contains [resources](#) to aid in creating your own test images. These creation aids will be in the form of interesting data files, useful software tools and procedures for specific tasks.

IMPORTANT NOTE: This web site is under development and may change or be reorganized at any time.

Data Set Types

There are several uses envisioned for the data sets, but we also expect that there will be unforeseen applications. The four most obvious applications are testing forensic tools, establishing that lab equipment is functioning properly, testing proficiency in specific skills and training laboratory staff. Each type of data set has slightly different requirements. Most data sets can be used for more than one function. For example, the **Russian Tea Room** can be used to evaluate the behavior of a tool to search UNICODE text or display UNICODE text. This set can also be used as a skill test for an examiner to demonstrate proficiency in working with UNICODE text or as a training exercise.

Data sets for tool testing

Data sets for tool testing need to be completely documented. The user of the data set needs to know exactly what is in the data set and where it is located. These data sets should also provide specification for a set of explicit tests. However, the user should have sufficient documentation to develop and execute other test cases if necessary or desirable. These data sets could be part of a realistic investigation scenario, but it is easier to control expected results if each data set is focused on a particular type of tool function. Examples of focused function areas are string searching, deleted file recovery and email extraction.

11

There will tend to be many small test images, each focused on a particular feature for the tool fu

<https://www.cfreds.nist.gov/>

R これは人材育成としてアリか？

- 自学自習という意味ではよいと思う
- ただし、単にコレをやるだけではハードルが高すぎないか？
- 必要なツールがすぐわかるか 使い方は
- そもそも必要な基礎知識がかなり多い
- なので段階を踏むためにも適当に簡単にした題材がたくさん必要？
- 実務向け技術として
dd / pcap分析だけで十分か？

R 日本でやる際の問題

- ツールの問題
 - 日本語で利用可能なフリーのツールが足りないのではないか
 - 例えばよくあるForensic用Linux distributionは日本語版がイマイチ
 - Autopsyの日本語化をもう少しちゃんとしないと
- 特にWindowsを含むdd imageのライセンス問題はどうか
 - Fair useがない国ならではの問題？
 - おそらく適切なライセンスがあるはずだが個別相談になりかねない…

R これらをクリアしつつ…？

- 日本版DFコンテストを企画したい
- 必要なもの
 - それなりに意味があるインシデントシナリオ
 - それにそったimageの作成
 - ライセンス問題の解決
 - 解決できなかつたらLinux版だけやってみる
 - ツール情報の提供
 - 可能なら日本語化
- やったら参加いただけますか…？