Digital Forensics and Incident Response (DFIR) Workshop

"first step against cybercrime"

ALI HADI
Princess Sumaya University for Technology
Computer Science Dept.
October 10, 2017

Abstract

Crime committed on computers or information stored on computers is rapidly increasing, especially when our daily lives have become more reliant on devices and digital information. This "Digital Forensics and Incident Response" workshop will focus on two of the most critical fields in all of information security.

It will help participants gain both the theoretical and practical skills required to perform digital forensic investigations and respond to computer incidents, by applying hands-on experience with real-world scenarios. The goal of the workshop is to inspire the interest of participants with diverse backgrounds, spread the awareness of fighting cybercrime, and build a better DFIR community.

Keywords: Digital Forensics, DFIR, Incident Response, Investigation

Description

The Digital Forensics and Incident Response Workshop focuses on identifying, investigating, and remeidating computer network exploitation. DFIR[1] is a broad field and this workshop will serve as your first step in fighting against cyber crime. In particular, it will show and cover the following:

- Introduction to Digital Forensics and Incident Response,
- Trending Research Areas,
- Disk Imaging, Mounting, and Verification,
- File Carving and File analysis,
- Working with Autopsy, Searching and indexing,
- Analyzing Internet history, Thumbnails and Prefetch Files,
- Basic Windows Registry Analysis,
- Generating Reports,
- Extra: Performing Basic DFIR Triage from Collection to Analysis.

Requirements for the participants

To be able to participate in the hands-on sessions during the workshop you will need a Laptop with your prefered operating system and a virtual machine hypervisor such as Virtualbox[2] or VMWare[3] installed. You will need to download a Windows VM (preferably 7/8)[4], and the CyLR CDQR Forensics Virtual Machine (CCF-VM)[5]. Finally, you will also need to download a number of digital forensic tools. The full list will be announced one week before the workshop.

Provided materials

The material and all the instructions will be publicly available on a dedicated Github repository. The repository will be announced at the workshop. You are invited to contribute, open issues and ask questions there after the workshop. The final materials will be published after the workshop day.

[1] https://medium.com/@sroberts/introduction-to-dfir-d35d5de4c180
[2] https://www.virtualbox.org/
[3] https://www.vmware.com/
[4] https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
[5] https://github.com/rough007/CCF-VM

Timetable

- **9:00-10:00** Introduction to Digital Forensics and Incident Response, Trending Research Areas,
- **10:00-10:30** Data acquisition and Verification,
- **10:30-11:00** Hands-on: Disk Imaging, Mounting, and Hashing,
- **11:00-11:15** Coffee Break
- **11:15-11:30** File Carving and File Analysis
- **11:30-12:00** Hands-on: File carving, recovering deleted files, and file Analysis
- **12:00-13:00** Hands-on: Working with Autopsy, Searching and indexing,[6]
- **13:00-14:00** Lunch
- **14:00-14:30** Artifacts: Internet history, Thumbnails, Prefetch Files, Basic Windows Registry Analysis,
- **14:30-15:30** Hands-on: Analyzing Windows Forensic Artifacts
- **15:30-16:30** Extra: DFIR Triage: From Collection to Analysis.
- **16:30-17:00** Conclusions, Closing Remarks, Q&A Session

Outcomes

By the end of this workshop, attendees will:

- have good understanding of DFIR aspects and trending research areas,
- be able to perform data acquisition and verify data,
- know how to apply file carving techniques to recover deleted files and analyze acquired files,
- learn the essentials of working with Autopsy, and analyzing different Windows artifacts,
- have the ability to perform easy DFIR triage starting from data collection to analysis.

[6]There should be 20 minutes break for praying during this session.

About Presenter

Ali Hadi [7] *is an Information and Cyber Security Specialist with 14+ years of industrial experience in Information Technology (IT), currently working as a full time university professor and researcher for the Computer Science Dept., Princess Sumaya University for Technology. He provides consulting in several areas of security including digital forensics and incident response, cyber threat hunting, cyber threat intelligence, penetration testing, and vulnerability assessments. He is also an author, speaker, and freelance instructor. His research interests include digital forensics, incident response, cyber threat hunting, and cyber threat intelligence.*

[7] `https://www.ashemery.com/bio.html`