

Digital Corpora 2

By: Minh Dang, Jacky Chen, Ben Paorik, Sam lee Supervisor: Dr Dax Roberts Client: Paul Bryant

```
Command Prompt
05-29 02:10:32 UTC+0800
0xffff9e83f9e27800 dumpcap.exe 2184 5848 0 ----- 1 0 2020-05-29 02:16:48 UTC+0800 2020-
05-29 02:16:49 UTC+0800
0xffff9e83f7272500 taskhostw.exe 1312 368 4 0 1 0 2020-05-29 02:53:33 UTC+0800
0xffff9e8085174c0 logonUI.exe 7932 680 0 ----- 1 0 2020-05-29 04:22:08 UTC+0800 2020-
05-29 04:23:39 UTC+0800
0xffff9e83f72614c0 logonUI.exe 7652 690 0 ----- 1 0 2020-05-29 04:41:09 UTC+0800 2020-
05-29 05:10:13 UTC+0800
0xffff9e840845b300 svchost.exe 6588 648 2 0 0 0 2020-05-29 05:17:36 UTC+0800
0xffff9e83fc974c0 audiodg.exe 8188 1648 4 0 0 0 2020-05-29 05:20:27 UTC+0800
0xffff9e83f48a64c0 Taskmgr.exe 1280 1268 15 0 1 0 2020-05-29 05:21:28 UTC+0800
0xffff9e84084c2800 Generate bad.E 5684 1268 1 0 1 0 2020-05-29 05:26:43 UTC+0800
0xffff9e83f9e18800 keylogger.exe 4848 5684 1 0 1 1 2020-05-29 05:26:44 UTC+0800
0xffff9e83fbf7800 conhost.exe 7772 4848 3 0 1 0 2020-05-29 05:26:44 UTC+0800
0xffff9e83f9b0a4c0 cmd.exe 3332 1268 1 0 1 0 2020-05-29 05:27:17 UTC+0800
0xffff9e83fc9ab4c0 conhost.exe 4552 3332 5 0 1 0 2020-05-29 05:27:17 UTC+0800
```



Keylogger Found

Phishing Website

INTRODUCTION

Welcome to the end product of Digital Corpora 2. The goal was to create learning materials suitable for the education of future WeITec students. Our corpora contains items such as disk images, memory dumps, network packet captures and scenarios which students will work through and hopefully learn a thing or two.

The topic we have based our learning materials off of is phishing. It is a topic that we believe interests many IT students as they should have encountered or at least heard of the term before. The learning materials consist of developing a phishing attack, seeing how it works, and then obtaining the phished details in a text file. They will then analyse the attack and record their findings. We hope this will educate students about phishing as our aim is to help them get comfortable with industry-standard tools

DEVELOPMENT

The development cycle of this project was run through a Waterfall development approach. technical development was done using VMware workstation pro to run and develop our VMs. This would also serve as the place the project scenarios would run. The environment is Windows 10 based with a Windows Server 2012 R2 acting as an email server for the phishing attack. Some notable tools incorporated include, Wireshark, Volatility Framework and Autopsy. Each tool serves a purpose in both scenarios one and two. Through the development process, we hit early issues around COVID-19 as all teams did. This meant our

homes became our workplaces which we were forced to adapt to. Our first technical issue was configuring our local email connectivity but soon resolved that and proceeded through the workload faster than anticipated this resulted in us creating a second scenario further developing on the skills taught in scenario 1. Our client expressed his interest in having the learning materials be suitable for Level 6 Information technology students, this meant we had to look at tools we knew they would have experience with and build upon that. As well as incorporating industry toolchains, we believe that experience with these toolchains is beneficial to a student's learning and can provide them with an edge when they enter the industry.

CONCLUSION

In the end our project achieved its goal of creating learning materials suitable for level 6 students, we believe that we achieved what the client had tasked us with at the beginning of the project. In the end we produced two scenarios, one about email phishing and the second but more importantly as a development team we have come out of this experience with a greater understanding of working within a cohesive team dynamic and being proud of the work that we were producing.