USC University of Southern California

OFFICE OF RESEARCH
Randolph W. Hall
Vice President of Research
vpres@usc.edu

June 21, 2019

Dr. Hao Li
Computer Science
University Park Campus
SAL 300 MC 0781

Dear Dr. Li,

As you are aware the University has conducted an inquiry into allegations of research misconduct against you and has determined that an investigation is warranted. According to the University Policy on Scientific Misconduct (see attached) the subject of an allegation has the duty to furnish data, records and other documents as requested by the university so that a thorough review can be completed. The destruction, absence of, or any failure to provide research records adequately documenting the questioned research at any point in the process is evidence of research misconduct where it is established by a preponderance of the evidence that the subject of an allegation intentionally, knowingly, or recklessly had research records and destroyed them, had the opportunity to maintain the records but did not do so, or maintained the records and failed to produce them in a timely manner, and that the subject's conduct constitutes a significant departure from accepted practices (Policy 4.1.4).

The Investigation Committee has requested access to your laptop and any other hard drives (e.g., group servers, on the cloud or elsewhere) where the program codes relevant to the allegations being reviewed (see attached) may be found. You may do so in person. All hard drives will be immediately copied and returned to you. Please provide the requested items and any other materials you think would be relevant to the Committee's investigation to the Office of the Vice President of Research by July 8. Non-compliance with this request will subject you to University Policy violations and appropriate disciplinary actions.

We appreciate your cooperation with this request.

Sincerely,

Randolph Hall, PhD
Vice President, Research

CC: Dr. Kristen Grace, USC Research Integrity Officer

Institute of Creative Technologies (ICT)
Dr. Hao Li

Information Security Summary

July 8, 2019

Rob Groome – Director of Security Operations
Alan Hong – Senior Incident Response Analyst

Privileged and Confidential

USC University of Southern California

Office of Compliance
University of Southern California
Los Angeles, CA 90089

Dear Dr. Grace,

We have completed our analysis of the MacBook Pro with Serial Number C02V20C9J93D. Our engagement was performed in accordance with our Incident Request Number, REQ0131116, and our procedures were as follows:

- Image the device
- Locate items of interest(s)
- Provide any further assistance you may need

The procedures and findings from our initial analysis are provided in this report.

We appreciate the cooperation and assistance provided to us during the course of our work. If you have any questions, please feel free to reach out to us.

Kind regards,
USC Information Security Office

Table of Contents

Executive Summary

History/Background

- On June 21, 2019, Rob Groome informed me, Alan Hong, about the need to acquire a device for an investigation for the Office of Compliance. Details of the data size were later revealed to provide an approximate time it would take to forensically image the device(s) and return them to the owner. Furthermore, details of evidence drop off were also discussed.
- Communications between the Information Security Office and the Office of Compliance has primarily been done over email with a few phone calls for verification purposes on scheduling
- Dr. Grace and Dr. Li both agreed to meet at the Carole Little Building on June 27, 2019 at 10:00 AM for the evidence hand off
- The only evidence that was presented and handed over with Dr. Grace present to witness, was the MacBook Pro with Serial Number C02V20C9J93D
- Chain of Custody documentation was filled out and the imaging process commence the same day June 27, 2019 at approximately 10:45 AM.

Findings

- It was discovered that the machine contains very little data and appears to have been recently re-imaged. The relevant data that was located was the exact folder that Dr. Li mentioned that he copied from his external hard drive to the laptop.
- The following is a summary of the important items/artifacts/information to gain a better understanding of the laptop:
    - The earliest system file times are all documented to be 2019-06-24 at 23:01:56 (PDT)
    - Internet History, Cookies, and Cache were all bare and contained little to no information
    - The User Account that was created for him by the “IT Group” to use, pinscreen, had a creation time of 2019-06-24 at 23:33:14 (PDT)
    - The SIGAsia17 Directory had the Date Modified as 2019-06-26 at 09:54:59 (PDT)

Scope and Analysis Considerations

This report summarizes the Information Security Office's analysis and findings related to the areas of investigation. The Information Security Office's engagement was limited by the amount of data provided by Dr. Hao Li.

Dr. Hao Li Provided the following:

- Apple MacBook Pro – 15" – Serial Number C02V20C9J93D

Areas of Interest / Relevant Areas of Analysis

- User account creation
  - Pinscreen account was created on 2019-06-24 at 23:33:14 (PDT)
- System File creation
  - System file creation times start at 2019-06-24 at 23:01:56 (PDT)
- Internet/Browser History
  - Contained the opening pages and little history by going to GitHub
- Research Folder – SIGAsia17
  - Folder is confirmed to be in the location mentioned. The folder has 309,830 items
  - The folder was added to the computer on 2019-06-25 at 18:26:18 (PDT)
- Desktop / Documents / Downloads Folder
  - They were all empty and contained no data

Items that should be noted are:

- It should be noted that the laptop referenced above, is not an USC Asset but one that Dr. Hao Li presented and claimed all his work was on there
- Furthermore, the folder that was copied (SIGAsia17) all has last modified times pointing back to 2019-06-25 at 18:26:18 (PDT) which means we do not have the visibility into the original creation time because the items have been tampered with since the copy was made from another media source to this laptop.
- If possible, it would be best if we were able to obtain the original sources
- Dr. Li mentioned during the time of evidence drop off that the laptop was worked on by the "IT Group". It is currently unknown which "IT Group" this is.

From: Kristen Grace
To: Hao Li
Cc: Randolph W. Hall; Marty Levine; Rob Groome; Alan Hong
Subject: USC Mac Book Pro
Date: Tuesday, July 2, 2019 11:25:43 AM

Dear Dr. Li,

It has come to my attention that the laptop you dropped off to ITS last week was not, in fact, your ICT machine. We need you to drop off your university MacBook Pro with ICT tag "T06270" and serial of C02SXE11GTF1 to ITS tomorrow morning. Please let me know what time you will be arriving and I will have Alan available to collect and fill out the chain of evidence form.

Sincerely,
Kristen Grace

Kristen Grace, M.D., Ph.D.
Research Integrity Officer
Office of Research

University of Southern California
3720 S Flower Street, Suite 325
(213) 821 7297
gracekri@usc.edu

Institute of Creative Technologies (ICT)
Dr. Hao Li

Information Security Summary

July 29, 2019

Rob Groome – Director of Security Operations
Alan Hong – Senior Incident Response Analyst

Privileged and Confidential

USC University of Southern California

Office of Compliance
University of Southern California
Los Angeles, CA 90089

Dear Dr. Grace,

We have completed our analysis of the following items:

- MacBook Pro with Serial Number C02V20C9J93D
- MacBook Pro with Serial Number C02SXE11GTF1
- Western Digital Elements External Hard Drive with Serial Number WXS1EC7EKWMF

Our engagement was performed in accordance with our Incident Request Number, REQ0131116, and our procedures were as follows:

- Image the device
- Locate items of interest(s)
- Provide any further assistance you may need

The procedures and findings from our initial analysis are provided in this report.

We appreciate the cooperation and assistance provided to us during the course of our work. If you have any questions, please feel free to reach out to us.

Kind regards,
USC Information Security Office

Table of Contents

Executive Summary

History/Background

- On June 21, 2019, Rob Groome informed me, Alan Hong, about the need to acquire a device for an investigation for the Office of Compliance. Details of the data size were later revealed to provide an approximate time it would take to forensically image the device(s) and return them to the owner. Furthermore, details of evidence drop off were also discussed.
- Communications between the Information Security Office and the Office of Compliance has primarily been done over email with a few phone calls for verification purposes on scheduling
- Dr. Grace and Dr. Li both agreed to meet at the Carole Little Building on June 27, 2019 at 10:00 AM for the evidence hand off
- The only evidence that was presented and handed over with Dr. Grace present to witness, was the MacBook Pro with Serial Number C02V20C9J93D
- Chain of Custody documentation was filled out and the imaging process commenced the same day June 27, 2019 at approximately 10:45 AM.
- Further communications occurred and there was an agreement that Dr. Li would bring his ICT assigned laptop for imaging as well as the external hard drive that contained the original research.
- Dr. Li handed over a MacBook Pro with Serial Number C02SXE11GTF1 and a Western Digital Elements External Hard Drive with Serial Number WXS1EC7EKWMF on July 10, 2019 and imaging commenced the same day.
- After imaging and verification of data, the devices were returned to Dr. Li on July 15, 2019.

Findings

- MacBook Pro with Serial Number C02V20C9J93D
    - It was discovered that the machine contains very little data and appears to have been recently re-imaged. The relevant data that was located was the exact folder that Dr. Li mentioned that he copied from his external hard drive to the laptop.
    - The following is a summary of the important items/artifacts/information to gain a better understanding of the laptop:
        - The earliest system file times are all documented to be 2019-06-24 at 23:01:56 (PDT)
        - Internet History, Cookies, and Cache were all bare and contained little to no information
        - The User Account that was created for him by the “IT Group” to use, pinscreen, had a creation time of 2019-06-24 at 23:33:14 (PDT)
        - The SIGAsia17 Directory had the Date Modified as 2019-06-26 at 09:54:59 (PDT)

- MacBook Pro with Serial Number C02SXE11GTF1
    - It was discovered that the machine had two separate partitions[1] on the computer and it was running both macOS and Windows 10 Enterprise. The same scenario, recent

[1] Partitions can typically be referenced as logical separations of a hard drive. This allows for the installation of multiple Operating Systems on a single hard drive in this scenario.

imaging, appears to have also taken place with both partitions as the date stamps all traverse back to 2016/2017 activity and nothing recent.

- macOS Partition
  - The last event that occurred documented to 2016-01-01 at 14:10:43 (PDT) which was attributed to JAMFAgent, which is an imaging software.
  - There were 4 user accounts that were located: Administrator, bullfrog, li, shared. On all accounts the Desktop, Documents, Downloads directories were all empty
- Windows Partition – Windows 10 Enterprise
  - The system's last timestamp of change is 2017-01-17 at 15:42:09 (PDT)
  - There were 4 user accounts that were located: bullfrog, defaultuser0, ict, and public. All of which the directories of Desktop, Document, and Downloads were empty

- Western Digital Elements External Hard Drive with Serial Number WXS1EC7EKWMF
  - The hard drive was a 4TB external hard drive in which 115 GB was utilized.
  - This was a storage drive and per the previous engagement with Dr. Li, the directory of interest was labeled "SIGAsia17". The directory had the following attributes:
    - Date Created - 2019-06-24 at 10:47:16 (PDT)
    - Date Modified - 2019-06-24 at 10:47:16 (PDT)
    - Date Accessed - 2019-07-09 at 15:49:52 (PDT)

Scope and Analysis Considerations

This report summarizes the Information Security Office's analysis and findings related to the areas of investigation. The Information Security Office's engagement was limited by the amount of data provided by Dr. Hao Li.

Dr. Hao Li Provided the following:

- Apple MacBook Pro – 15" – Serial Number C02V20C9J93D
- Apple MacBook Pro – 15" – Serial Number C02SXE11GTF1
- Western Digital Elements External Hard Drive – Serial Number WXS1EC7EKWMF

Areas of Interest / Relevant Areas of Analysis

- Apple MacBook Pro – 15" – Serial Number C02V20C9J93D
    - User account creation
        - Pinscreen account was created on 2019-06-24 at 23:33:14 (PDT)
    - System File creation
        - System file creation times start at 2019-06-24 at 23:01:56 (PDT)
    - Internet/Browser History
        - Contained the opening pages and little history by going to GitHub
    - Research Folder – SIGAsia17
        - Folder is confirmed to be in the location mentioned. The folder has 309,830 items
        - The folder was added to the computer on 2019-06-25 at 18:26:18 (PDT)
    - Desktop / Documents / Downloads Folder
        - They were all empty and contained no data
- Apple MacBook Pro – 15" – Serial Number C02SXE11GTF1
    - Running macOS and a Bootcamp partition. Both partitions have system dates pointing back to 2016 and 2017 which means that there is a high possibility that the Operating System(s) has been recently re-imaged.
        - macOS Partition
            - The last event that occurred documented to 2016-01-01 at 14:10:43 (PDT) which was attributed to JAMFAgent, which is an imaging software.
            - The Operating System Version was running macOS Sierra version 10.12.2. Which is an outdated version as of the current writing of this report, the most recent version Apple Inc has released is 10.14.5
            - There were 4 user accounts that were located: Administrator, bullfrog, li, shared. The Desktop, Documents, Downloads directories on all 4 accounts were all empty
        - Windows Partition
            - The system's earliest timestamp is 2017-01-17 at 12:22:54 (PDT)
            - The system's last timestamp of change is 2017-01-17 at 15:42:09 (PDT)
            - The operating system is running Windows 10 Enterprise
            - There were 4 user accounts that were located: bullfrog, defaultuser0, ict, and public. All of which the directories of Desktop, Document, and Downloads were empty

- Western Digital Elements External Hard Drive – Serial Number WXS1EC7EKWMF
    - The hard drive was a 4TB external hard drive in which 115 GB was utilized.
    - This was a storage drive and per the previous engagement with Dr. Li, the directory of interest was labeled "SIGAsia17". The directory had the following attributes:
        - Date Created - 2019-06-24 at 10:47:16 (PDT)
        - Date Modified - 2019-06-24 at 10:47:16 (PDT)
        - Date Accessed - 2019-07-09 at 15:49:52 (PDT)
        - Contains 4 folders (then each folder has a lot of their own details):
        - hair_data
            - Date Created - 2018-09-28 at 11:29:42 (PDT)
            - Date Modified - 2019-07-09 at 11:29:51 (PDT)
            - Date Accessed - 2019-07-09 at 15:50:03 (PDT)
        - hair_database
            - Date Created - 2018-09-28 at 09:58:17 (PDT)
            - Date Modified - 2018-09-28 at 11:19:41 (PDT)
            - Date Accessed - 2019-07-09 at 15:50:00 (PDT)
        - inputs
            - Date Created - 2017-03-05 at 02:02:16 (PDT)
            - Date Modified - 2018-10-20 at 20:56:13 (PDT)
            - Date Accessed - 2019-07-09 at 15:49:56 (PDT)
        - siga17
            - Date Created - 2018-09-26 at 16:18:47 (PDT)
            - Date Modified - 2018-09-26 at 17:29:17 (PDT)
            - Date Accessed - 2019-07-09 at 15:49:55 (PDT)

Items that should be noted are:

- It should be noted that the MacBook Pro with Serial Number C02V20C9J93D, is not an USC Asset but one that Dr. Hao Li presented and claimed all his work was on there
- Furthermore, the folder that was copied (SIGAsia17) all has last modified times pointing back to 2019-06-25 at 18:26:18 (PDT) which means we do not have the visibility into the original creation time because the items have been tampered with since the copy was made from another media source to MacBook Pro with Serial Number C02V20C9J93D.
- Dr. Li mentioned during the time of evidence drop off (June 27, 2019) that the laptop was worked on by the "IT Group". It is currently unknown which "IT Group" this is.
- The MacBook Pro with Serial Number C02SXE11GTF1, contains 2 partitions and both Operating Systems did not have any recent data and all system times points to a historical time space. Although we are unable to determine the exact date of when imaging occurred, it can be said that the action took place prior to the relinquishment of the machine.
- The external hard drive appears to have the relevant data for further queries and analysis.