SANS FOR518 - Mac Forensic Analysis Challenge Answers

Challenge Answers

This debrief does not contain every forensic artifact that this data could be found but should provide a good starting point to see what was missed during the initial triage provided during the final challenge timeframe.

1. **What types of computers and devices have been seized?**

David Lightman

- Laptop
    - OS Version: 10.13.1 (/System/Library/CoreServices/SystemVersion.plist)
    - Model: MacBookPro11,1 (/Library/Preferences/SystemConfiguration/NetworkInterfaces.plist)
    - IP Address: DHCP (/Library/Preferences/SystemConfiguration/preferences.plist) 10.199.0.123 [@Hyatt_WiFi] (/private/var/db/dhcpclient/leases/*)
    - Time Zone: America/Los Angeles (/private/etc/localtime, Metadata)

Jennifer Mack

- iPhone
    - OS Version: 11.0.1 (/mobile/Library/Logs/AppleSupport/general.log)
    - Model: iPhone 7,2 (/mobile/Library/Logs/AppleSupport/general.log))
    - Serial Number: DNPNDLQSG5MH
    - IP Address: DHCP – 192.168.101.109 (CrystalPalace)
        - ICCID – 8901260932773426051 (/wireless/Library/Preferences/com.apple.commcenter.plist)
    - Phone Number: 1-571-457-8083 (/wireless/Library/Preferences/com.apple.commcenter.plist)

Dr. Stephen Falken

- Laptop
    - OS Version: 10.13.2
    - Model: MacBookAir5,1
    - IP Address: DHCP – 10.199.29.68 [@Hyatt_WiFi]
    - Time Zone: America/Los Angeles

2. **What accounts and/or aliases are associated with each user?**

David Lightman

- aka dlightman (username)
- d.l1ghtm4n@gmail.com (/Users/dlightman/Library/Accounts/Accounts4.sqlite)
    - Gmail Email. Apple ID
    - *Note: Account d.lightman@gmail.com was accidentally put into the accounts, however it did not work.*

- Dlightful Man
    - WhatsApp
    - /mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite
    -
- 1-571-457-8084
    - Cellular, WhatsApp
    - /mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite

Jennifer Mack

- 1337jmack@gmail.com
    - Gmail, Apple ID
- Jmack
    - WhatsApp
    - /mobile/Applications/group.net.whatsapp.WhatsApp.shared/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist
- 1-571-457-8083
    - Cellular, WhatsApp
    - /mobile/Applications/group.net.whatsapp.WhatsApp.shared/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist
    - /wireless/Library/Preferences/com.apple.commcenter.plist
- "jm" & 1337jm (@protonmail.com)
    - ProtonMail
    - /mobile/Applications/group.ch.protonmail.protonmail/Library/Preferences/group.ch.protonmail.protonmail.plist

Dr. Stephen Falken

- drfalken (username)
- drfalkenstephen@gmail.com
    - Gmail, Apple ID

3. **Who is communicating and how?**

- Regular Email
    - David & Jen
        - /private/var/mobile/Library/Mail/IMAP-1337jmack@gmail.com@imap.gmail.com/INBOX.imapmbox/*
        - /Users/dlightman/Library/Mail/V5/8E359999-5616-4625-B74F-46E812760213/[Gmail].mbox/All Mail.mbox/*
    - Jen and Jerry Lawson
        - /private/var/mobile/Library/Mail/IMAP-1337jmack@gmail.com@imap.gmail.com/INBOX.imapmbox/*
- iMessage/SMS
    - David & Jen
    - /Users/dlightman/Library/Messages/*.ichat, chat.db
    - /mobile/Library/SMS/sms.db
- FaceTime/Cellular
    - David & Jen
    - /private/var/mobile/Library/CallHistoryDB/CallHistory.storedata

- Protonmail
    - Jen and Jerry Lawson
    - /private/var/mobile/Library/Mail/IMAP-1337jmack@gmail.com@imap.gmail.com/INBOX.imapmbox/*
- WhatsApp
    - David & Jen
    - /mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite

4. **Has anyone done any traveling?**

David Lightman:

- Arlington, VA
- Washington, DC
- London, England
- Bletchley, England
- Merrifield, VA
- San Diego, CA

- Photos & Videos Metadata
- Wi-Fi History – /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
- W-Fi Location Database - /private/var/folders/zz/zyxvpxvq6csfxvn_n00000sm00006d/C/cache_encryptedA.db

Jennifer Mack:

- Washington, DC
- London, UK
- Heathrow Airport
- Arlington, VA
- Dulles Airport
- San Francisco, CA
- San Diego, CA

- Photos & Videos Metadata
- Wi-Fi History – /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
- W-Fi Location Database - /private/var/folders/zz/zyxvpxvq6csfxvn_n00000sm00006d/C/cache_encryptedA.db

Dr. Stephen Falken:

- London, UK
- Arlington, VA
- Dulles Airport
- San Francisco, CA
- San Diego, CA

- Wi-Fi History – /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
- W-Fi Location Database - /private/var/folders/zz/zyxvpxvq6csfxvn_n00000sm00006d/C/cache_encryptedA.db
- Logs: (correlate with other activities) - /private/var/log/daily.out

5. **Is there any malware on the systems?**

- Red Herrings:
  - Dr. Falken installed MacKeeper (amongst other shady software) which may/may not be malware depending on which website you review. Its more or less a Potentially Unwanted Application (PUA).
  - David Lightman installed various keyloggers onto his system to "test" them.
  - David Lightman also tested the Bella RAT that was later installed onto Dr. Falken's system.

- Jen did recon on Dr. Falken
  - Followed him to San Francisco, CA
  - Communicated with Jerry Lawson over SMS and Protonmail
- Jen and Dr. Falken came back to Arlington, VA
- 05/08/2018 - Jen acquired pvsupport.dmg from Jerry Lawson via ProtonMail. Jen AirDrop'ed it to David.
- 05/08/2018 - David prepared USB drive with pvsupport.dmg on it, named it ProtovisionSupport.
- 05/09/2018 - Got into Protovision by acting as tech support for Wi-Fi. Got onto Protovision network with company provided credentials.
- Inserted ProtovisionSupport USB drive onto Dr. Falkens system, opened encrypted pvsupport.dmg copied contents onto system in Dr. Falken's home directory via Terminal and executed python install program 'pvsupport'. (Original install executable was automatically removed from system upon installation.)
  - Files included Bella Remote Access Trojan:
    - Persistence Launch Agent: /Users/drfalken/Library/LaunchAgents/com.apple.ncplugin.wifiagent.plist
    - Malware Binary: /Users/drfalken/Library/Containers/com.apple.wifiagent/Bella
      - Open Source Python Based RAT created especially for this system.
      - Calls back to Command and Control (192.168.100.101, David's system on Protovision network) on port 4545.
    - Malware Database: /Users/drfalken/Library/Containers/com.apple.wifiagent/bella.db
- David left Protovision but was still on their network (outside the office), and was able to use Bella RAT to acquire screenshots, username/password for Dr. Falken, Safari history, etc from Dr. Falkens system.
  - Bella Log and Exfiled Data: /Users/dlightman/Downloads/c2/Logs/Drs-MacBook-Air/drfalken/ & drfalken.txt
  - David ran 'Control Center.py' to launch the C2 server.
- Provided Dr. Falkens' credentials to Jen for use later via chat messages.
- Jen, David and Dr. Falken travel to San Diego, Ca.
- 05/13/2018-05/14/2018 - Dr. Falken received the file research_docs.zip from "Protovison Games" via AirDrop (assume a business associate). He unzipped it minutes later.
- While in the Grand Hyatt, Jen got access to and logged into Dr. Falkens system using his credentials. Jen saved the research_docs directory to an encrypted external volume "AppleSupport" that was created on David's system.
- Jen/David saved these documents to David's system. Zipped them up into a different research_docs.zip file. David then AirDrop'ed them to Jen's iPhone.
- Jen attempted to send research_docs.zip to Jerry Lawson via SMS, it failed. Jen then sent the zip file via ProtonMail.

6. **Can you provide any passwords?**

David Lightman

- Keychain/Login password – galagastillrocks
    - Should have asked instructor for password (passwords were known since memory images were captured.)
- Encrypted External Volume "AppleSupport" – protovision
- iOS Backup – galagaftw
- Encrypted DMG Volume "kl2.dmg" – tetris
    - "Password is my favorite block game" in chat with Jen
- Encrypted DMG Volume "pvsupport.dmg" - washingtondc

Dr. Stephen Falken

- Keychain/Login password – gamesRfun
    - Found in SMS Chat between David and Jen – Extracted from Bella RAT password popup module.

7. **Has any data been moved between these systems?**

- "Research Docs" from "Protovision Business Associate" to Dr. Falken -> "AppleSupport" Encrypted USB -> David Lightman's System -> Zipped and Airdropped to Jen's iPhone -> Jerry Lawson via ProtonMail.
- Bella Log and Exfiled Data: /Users/dlightman/Downloads/c2/Logs/Drs-MacBook-Air/drfalken/ & drfalken.txt

8. **Are there any encrypted containers?**
    - kl2.dmg
    - pvsupport.dmg (on ProtovisionSupport External Volume)
    - AppleSupport Encrypted External Volume

9. **Is anyone else involved that should be investigated?**

- Jerry Lawson – likely person that hired David and Jen.

10. **Is there anything else of investigative interest on these systems and devices?**

You tell me! There is so much more to be found – a thorough analysis of these systems cannot be done with the time provided in class. Takes these files home and use them to further your Mac and iOS forensic skills, research items of interest, or use them to compare items with your current cases.

SANS FOR518 - Mac Forensic Analysis Challenge

Objectives

- Get ready to put your new Mac and iOS forensic analysis skills to the test!

Challenge Background

In May of 2018, a sting occurred in San Diego, CA to catch two individuals (David Lightman and Jennifer Mack) accused of hacking systems, stealing data, and spying on system owners. The victim in this case was Dr. Stephen Falken of Protovision Systems.

System images, memory dumps, and an iPhones was acquired, archived, and provided to your group for analysis. Interviews have been conducted with these individuals, but these have not been provided to you. Questions may be asked to your instructor about these interviews.

Investigative Questions

Law enforcement agents have provided your group with specific questions they would like answered:

1. What types of computers and devices have been seized?
   - System Models, Serial Numbers, IP addresses, Time Zone, etc.
2. What accounts and/or aliases are associated with each user?
   - Usernames
   - Email
   - Internet
   - Etc.
3. Who is communicating and how?
   - What are the relationships between these individuals?
4. Has anyone done any traveling?
5. Is there any malware on the systems?
   - If so, what did it do?
   - How did it get there?
6. Can you provide any passwords?
7. Has any data been moved between these systems?
8. Are there any encrypted containers?
9. Is anyone else involved that should be investigated?
10. Is there anything else of investigative interest on these systems and devices?