UNIVERSITY OF BALTIMORE

College of Public Affairs

CYFI 330 / 700 Mobile Forensics

Examination of a .plist file from an IOS device

Under the Guidance of

Melvin de la Cruz

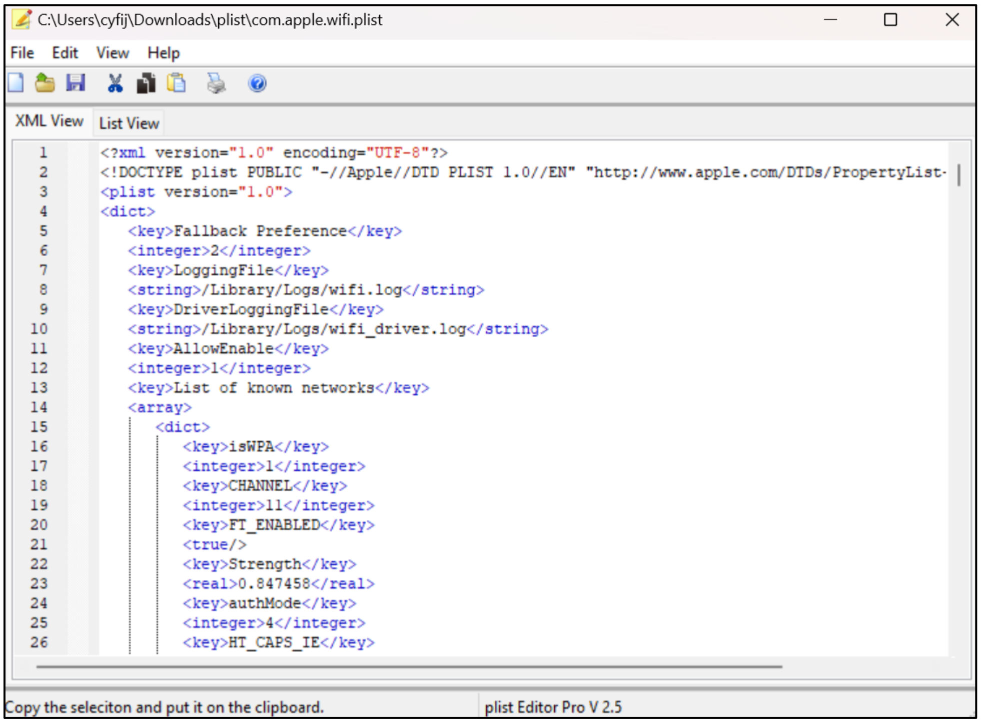
Assignment/Work by

Jeel Khatiwala

Examination of a .plist file from an IOS device

Instruction:

- **Download and Install pList Editor Pro and Extract plist.zip file.**
- **Open com.apple.wifi.plist file on pList Editor Pro.**



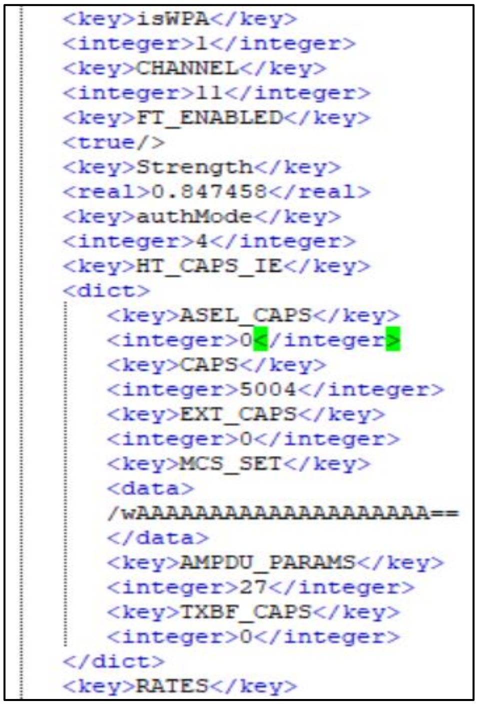
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-
<plist version="1.0">
<dict>
    <key>Fallback Preference</key>
    <integer>2</integer>
    <key>LoggingFile</key>
    <string>/Library/Logs/wifi.log</string>
    <key>DriverLoggingFile</key>
    <string>/Library/Logs/wifi_driver.log</string>
    <key>AllowEnable</key>
    <integer>1</integer>
    <key>List of known networks</key>
    <array>
        <dict>
            <key>isWPA</key>
            <integer>1</integer>
            <key>CHANNEL</key>
            <integer>11</integer>
            <key>FT_ENABLED</key>
            <true/>
            <key>Strength</key>
            <real>0.847458</real>
            <key>authMode</key>
            <integer>4</integer>
            <key>HT_CAPS_IE</key>
```

Copy the seleciton and put it on the clipboard.

plist Editor Pro V 2.5

- **Based on a review of the file's contents, what is contained within this plist file?**

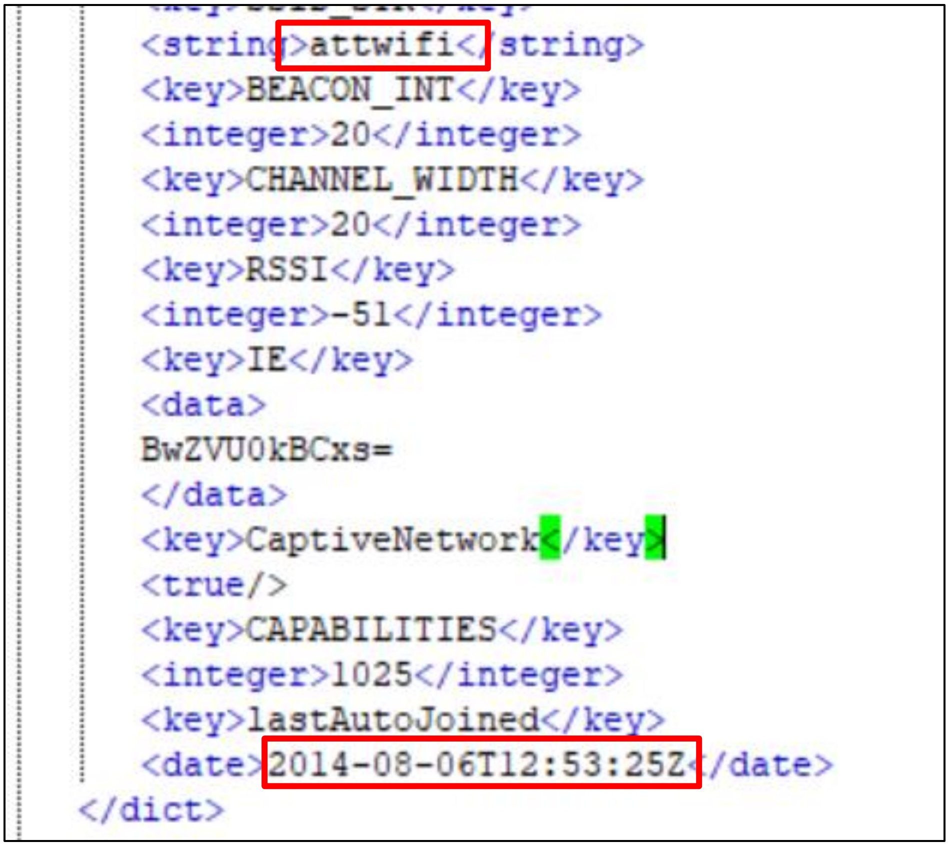
Answer: This file contains a list of all the wireless access points to which the IOS device connected.



```
<key>isWPA</key>
<integer>1</integer>
<key>CHANNEL</key>
<integer>11</integer>
<key>FT_ENABLED</key>
<true/>
<key>Strength</key>
<real>0.847458</real>
<key>authMode</key>
<integer>4</integer>
<key>HT_CAPS_IE</key>
<dict>
    <key>ASEL_CAPS</key>
    <integer>0</integer>
    <key>CAPS</key>
    <integer>5004</integer>
    <key>EXT_CAPS</key>
    <integer>0</integer>
    <key>MCS_SET</key>
    <data>
    /wAAAAAAAAAAAAAAAAAAAA==
    </data>
    <key>AMPDU_PARAMS</key>
    <integer>27</integer>
    <key>TXBF_CAPS</key>
    <integer>0</integer>
</dict>
<key>RATES</key>
```

- **Search through the plist file and identify the last time the IOS device connected to the wireless access point associated with starbucks or Bernes and Noble, i.e., attwifi?**

Answer: The IOS device last connected to attwifi on August 6, 2014 at 12:53:35 Zulu.

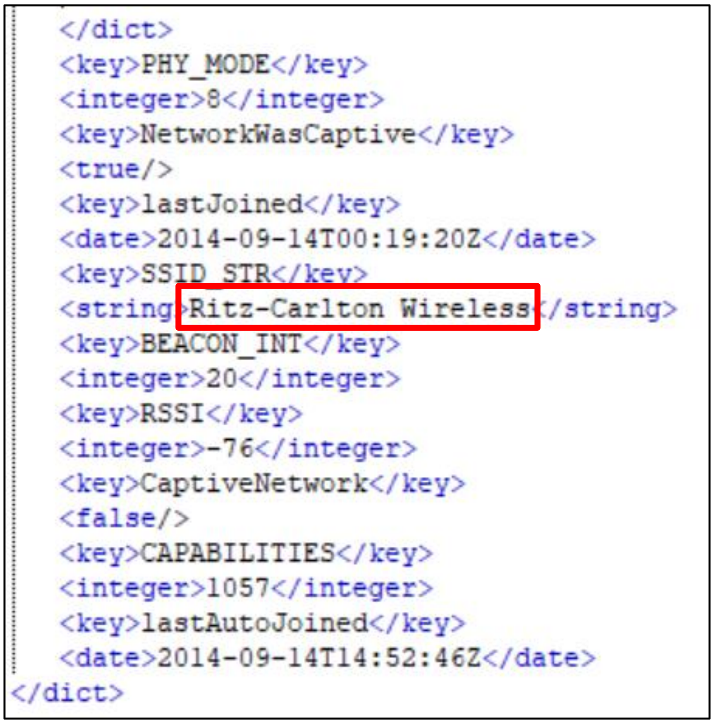


```
        <string>attwifi</string>
        <key>BEACON_INT</key>
        <integer>20</integer>
        <key>CHANNEL_WIDTH</key>
        <integer>20</integer>
        <key>RSSI</key>
        <integer>-51</integer>
        <key>IE</key>
        <data>
        BwZVU0kBCxs=
        </data>
        <key>CaptiveNetwork</key>
        <true/>
        <key>CAPABILITIES</key>
        <integer>1025</integer>
        <key>lastAutoJoined</key>
        <date>2014-08-06T12:53:25Z</date>
    </dict>
```

Additional Exercise:

- **To what network did the IOS device connect on September 14, 2014, at 14:52 Zulu?**

Answer: Ritz-Carlton Wireless



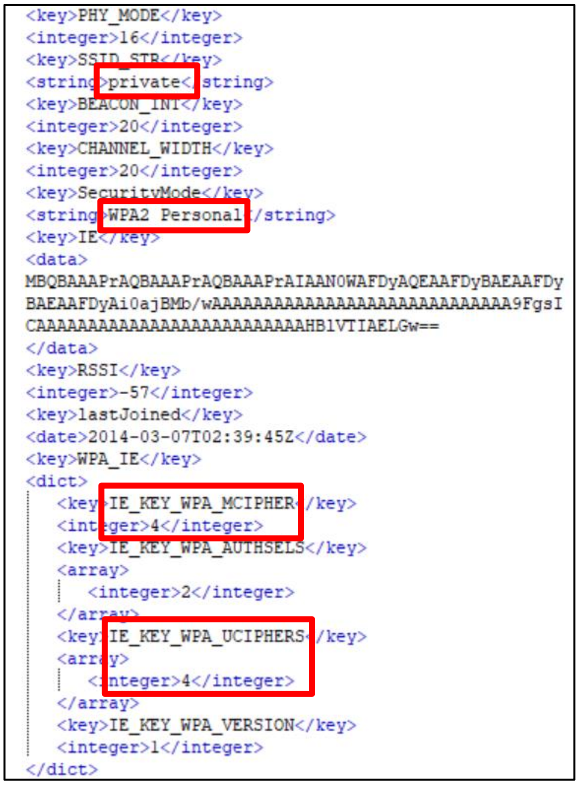
```
    </dict>
    <key>PHY_MODE</key>
    <integer>8</integer>
    <key>NetworkWasCaptive</key>
    <true/>
    <key>lastJoined</key>
    <date>2014-09-14T00:19:20Z</date>
    <key>SSID_STR</key>
    <string>Ritz-Carlton Wireless</string>
    <key>BEACON_INT</key>
    <integer>20</integer>
    <key>RSSI</key>
    <integer>-76</integer>
    <key>CaptiveNetwork</key>
    <false/>
    <key>CAPABILITIES</key>
    <integer>1057</integer>
    <key>lastAutoJoined</key>
    <date>2014-09-14T14:52:46Z</date>
</dict>
```

- **What type of encryption, if any, is used on the network using the SSID of private?**

Answer: WPA2 Personal with AES encryption for both

IE_KEY_WPA_MCIPHER is 4 - this means **AES** encryption.

IE_KEY_WPA_UCIPHERS is 4 - this means **AES** encryption.



```
<key>PHY_MODE</key>
<integer>16</integer>
<key>SSID_STR</key>
<string>private</string>
<key>BEACON_INT</key>
<integer>20</integer>
<key>CHANNEL_WIDTH</key>
<integer>20</integer>
<key>SecurityMode</key>
<string>WPA2 Personal</string>
<key>IE</key>
<data>
MBQBAAAPrAQBAAAPrAQBAAAPrAIAAN0WAFDyAQEAAFDyBAEAAFDy
BAEAAFDyAi0ajBMb/wAAAAAAAAAAAAAAAAAAAAAAAAAAAAA9FgsI
CAAAAAAAAAAAAAAAAAAAAAAAAAAHB1VTIAELGw==
</data>
<key>RSSI</key>
<integer>-57</integer>
<key>lastJoined</key>
<date>2014-03-07T02:39:45Z</date>
<key>WPA_IE</key>
<dict>
    <key>IE_KEY_WPA_MCIPHER</key>
    <integer>4</integer>
    <key>IE_KEY_WPA_AUTHSELS</key>
    <array>
        <integer>2</integer>
    </array>
    <key>IE_KEY_WPA_UCIPHERS</key>
    <array>
        <integer>4</integer>
    </array>
    <key>IE_KEY_WPA_VERSION</key>
    <integer>1</integer>
</dict>
```