Resources

1) Download Autopsy:

https://www.autopsy.com/download/ (https://www.autopsy.com/download/) (The write-up uses Autopsy 4.8.0)

2) Download IDA Pro Free:

https://www.hex-rays.com/products/ida/support/download.shtml (https://www.hex-rays.com/products/ida/support/download.shtml) (The write-up uses IDA Pro Free 5.0)

3) Download Wireshark:

https://www.wireshark.org/download.html (https://www.wireshark.org/download.html) (The write-up uses Wireshark 3.0.2.0)

4) Download Sublime Text:

https://www.sublimetext.com/3 (https://www.sublimetext.com/3) (The write-up uses Sublime Text 3)

6) CyberChef:

https://gchq.github.io/CyberChef/ (https://gchq.github.io/CyberChef/)

7) Convert Base64 to PNG:

https://onlinepngtools.com/convert-base64-to-png (https://onlinepngtools.com/convert-base64-to-png)

8) Decompile Jar File:

http://www.javadecompilers.com/ (http://www.javadecompilers.com/)

9) IDA Videos:

https://www.youtube.com/watch?v=vb18UVF4a_o (Part 1: https://www.youtube.com/watch?v=vb18UVF4a_o)

https://www.youtube.com/watch?v=tVvYsFStPTc (Part 2: https://www.youtube.com/watch?v=tVvYsFStPTc)

https://www.youtube.com/watch?v=kXSW4i0En_Y (Part 3: https://www.youtube.com/watch?v=kXSW4i0En_Y)

https://www.youtube.com/watch?v=rlhh4WiXyw0 (Part 4: https://www.youtube.com/watch?v=rlhh4WiXyw0)

10) Download Exiftool:

https://www.sno.phy.queensu.ca/~phil/exiftool/install.html (https://www.sno.phy.queensu.ca/~phil/exiftool/install.html)

11) Volatily Commands Cheat

https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf (https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf)

11) Volatily Commands Cheat

https://sourceforge.net/projects/pyinstallerextractor/ (https://sourceforge.net/projects/pyinstallerextractor/)