Since this is the first time I’ve used bulk\_extractor, and know very little about it, I’ve decided to have it collect everything it can find then later look for what is relevant with bulk\_extractor –e all –o ./bulkOut ./Week2-1.vmem

**1.) What is Jess’s email address?**

From more ./email.txt | grep –i jess, I found a lot of rjessica991@gmail.com. Since all I know about the target is the name “jess”, I’m guessing this is the one.

**2.) What is Jess’s Facebook page?**

From more ./url.txt | grep –i face, I was able to pick out a candidate which is http://www.facebook.com/profile.php?id=100001686984806. After pasting this link into the browser, it redirected me to a Jessica Runner Facebook account at https://www.facebook.com/jessica.runner.33, which matches the email username rjessica991 (Runner Jessica)

**3.) Are there any passwords in the memory image?**

I found a couple of them but not sure if they are genuine. I ran strings ./Week2-1.vmem | grep pass=, and got 3 passwords of “oobeSystem”, “windowsPE”, and “specialize”. I also tried strings ./Week2-1.vmem | grep –iP ‘\.com&pass’, which usually covers many in memory web logins, but couldn’t find any. I assume they were all overwritten by other data. Instead of coming up with nothing, I decided to dump the hash passwords using the following.

vol.py –f ./Week2-1.vmem imageinfo

vol.py –f ./Week2-1.vmem –profile=Win7SP0x86 hivelist

vol.py –f ./Week2-1.vmem –profile=Win7SP0x86 –y 0x88a1c008 –s 0x8228d9d0 hashdump

I then copy the NTLM hash to be crack online. I get Sandy: ke$ha, and both Guest and Administrator with null passwords. After getting the host’s password, I played around with this command

strings ./Week2-1.vmem | grep –P ke.ha

I was able to pull up some interesting strings of “The password to my Hotmail account is: ke$ha4life” Worried of getting into trouble, I decide not to test the email and password combination on the Hotmail website, so I’m going to leave it at that.

**4.) Were there any web searches that would be pertinent to the investigation?**

I look at url\_histogram.txt, and found a couple of interesting web search

http://philadelphia.cbslocal.com/2012/02/15/delaware-woman-arrested-for-alleged-murder-for-hire-plot

http://abcnews.go.com/GMA/video/murder-hire-setup-michael-dippolito-moves-13883240

http://www.truecrypt.org/download/transient/e90e28a4df/TrueCrypt%20Setup%207.1a.exe

http://en.wikipedia.org/wiki/Contract\_killing

http://en.wikipedia.org/wiki/Contract\_killing#By\_country

http://en.wikipedia.org/wiki/Contract\_killing#Notes

http://www.huffingtonpost.com/2012/02/01/virginia-woman-pleads-guilty-murder-for-hire\_n\_1247561.html

http://www.ktvb.com/news/local/Meridian-man-involved-in-murder-for-hire-scheme-gets-15-years-1390600

http://www.nbcactionnews.com/dpp/news/region\_missouri/northland/target-of-alleged-murder-for-hire-plot-talks-about-ex-wife

http://en.wikipedia.org/wiki/Contract\_killing#See\_also

http://abcnews.go.com/US/houston-murder-hire-mistress-testifies-alleged-hit-mans/story?id=14863350

http://www.google.com/flights/gwsredirect?q

And some more from cat ./rfc822.txt | grep jess

Subject: Re: Meeting tonight<BR>&gt; From: rjessica991@gmail.com<BR>&gt; To: benbitdiddle@hotmail.com<BR>

The URL themselves explain that Dan is either a crime and mystery movie fan, or he’s trying to find out how to remove someone out of his life. In addition, the data found from rfc822.txt does give a big hint that Dan is meeting with Jess tonight. So I did another quick search with strings ./Week2-1.vmem | grep ‘Subject: Re: Meeting tonight’. I found another interesting info

“WHAT!!! YOU WANT ME TO MURSER MY WIFE? WHAT IS WRONG WITH YOU?!?! That is \*so\* not what I want to do! I don’t love her anymore, but I’m not killing anybody. You are sick!”

So, I guess Dan is off the hook for intent to kill, however, still don’t know where his wife is.

**5.) What is the computer's IP address?**

Since bulk\_extractor pulled out Pcap file, I think it would be the best source to start. By opening the Pcap file with Wireshark, I was able to conclude that the Window7 (VM) machine’s IP was 172.16.246.144/24

**6.) What are the MAC addresses of the associated computer and router?**

Using the same method previously, and from analysis I think this Pcap shows a clear communication from a Window7 VM with NAT interface enabled. The reason is both the DHCP, DNS and other type of IP communications were going through the 172.16.246.2 IP which is the default VM gateway setting for many VMs including VirtualBox. So the Window7 VM MAC is 00:0c:29:21:93:08, the router’s (VM/NAT) MAC is 00:50:56:ff:81:85.

**7.) What type of device does the non-VMware MAC belong to?**

Surprisingly, all the communication using IP protocol was from and to a VMWare VMs. Non VM MACs that I’ve found are Cisco 00:05:00:00:00:0a, which could be a router, and LexmarkI 00:04:00:00:00:0a, which could be a printer. There are many more non-VM MAC but I’m not sure what they are.

EquipTra 00:01:00:00:00:20

LexmarkI 00:04:00:00:00:0a

Zettamed 00:07:00:00:00:0a

Telemati 00:00:5c:40:40:40

Eltecele 00:00:5b:40:40:40