Forensics

Room link : https://tryhackme.com/room/forensics

Task 1

#1 verify hash

```
$ md5sum victim.raw
> ba44c4b977d28132faeb5fb8b06debce
```

#2 Whats is the OS of this Dump? (Just write OS name in small)

```
$ volatility -f victim.raw --profile=Win7SP1x64 imageinfo
> windows ( suggested profiles = win7/8 variants )
```

#3 Whats is the PID of SearchIndexer ?

```
$ volatility -f victim.raw --profile=Win7SP1x64 pslist | grep Search
> 2180 ( remove grep to see output layout)
```

#4 What is the last directory accessed by the user? (Just write last folder name as it is?)

```
$ volatility -f victim.raw --profile=Win7SP1x64 shellbags | sort -k 6
> deleted_files
```

Task 2

#1 There are many suspicious open port, which is it ?(protocol:port)

```
$ volatility -f victim.raw --profile=Win7SP1x64 netscan
>udp:5005
```

#2 Vads tag and execute protection are strong indicators of malicious processes, can you find which are they?

```
$ volatility -f victim.raw --profile=Win7SP1x64 malfind | grep Vad -B 1
> 1860;1820;2464
```

Task 3

In lats task you have identified malicious processes, so lets dig into them and find some IOC's. you just need to find them and fill the blanks (You may search them on VirusTotal for more details :)
[IOC = indicator of compromise]

=> we need to dump memory regarding those processes

```
$ volatility -f victim.raw --profile=Win7SP1x64 memdump --pid=1820,1860,2464 --dump-dir PIDdump
```

#1 'www.go****.ru' (write full url without any quotation marks)

```
$ strings 1820.dmp | grep 'www.go' | grep .ru
> www.goporn.ru
```

#2 'www.i****.com' (write full url without any quotation marks)

```
$ strings 1820.dmp | grep 'www.i' | grep .com
> www.ikaka.com
```

#3 'www.ic******.com'

```
$ strings 1820.dmp | grep 'www.ic' | grep .com
> www.icsalabs.com
```

#4 202.***.233.*** (Write full IP)

```
$ strings 1820.dmp | grep '202\....\.233'
> 202.107.233.211
```

#5 ***.200.**.164 (Write full IP)

```
$ strings 1820.dmp | grep '.200\....164'
> 209.200.12.164
```

#6 209.190.***.***

```
$ strings 1820.dmp | grep '209.190\....\....'
> 209.190.122.186
```

#7 What is an unique environmental variable of PID 2464

```
$ volatility -f victim.raw --profile=Win7SP1x64 envars --pid=2464,1820,1860 |
sort -k 4 #we don't know what unique means so I compared to "bad" pids
> OANOCACHE
```