Questions and Answers

Are there any unusual processes running and if yes, name them and explain your reasoning briefly.

- Name: svchost.exe, Process ID (Pid): 2152, Parent Process ID (PPid): 1472
- svchost.exe has been created by explorer.exe (Pid: 1472) (suggests having been opened by user click in Windows Explorer)
- All the other svchost.exe are regulary created by services.exe (Pid: 496) and therefore have the PPid 496

```
# vol.py -f /mnt/hgfs/Temp/memdump.mem --profile Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
---snip---
 0xfffffa8002acfb10:explorer.exe                     1472   1360     34   1057 2019-07-18 01
. 0xfffffa8002781060:iexplore.exe                    3968   1472     15    676 2019-07-18 01
.. 0xfffffa8002a7e060:iexplore.exe                   4016   3968     39   1271 2019-07-18 01
.. 0xfffffa8002bd4710:iexplore.exe                   3080   3968     33   1187 2019-07-18 01
. 0xfffffa8001334360:FTK Imager.exe                  2976   1472     20    370 2019-07-18 01
. 0xfffffa800309e6c0:svchost.exe                     2152   1472      8     82 2019-07-18 01
. 0xfffffa8002c56b10:vmtoolsd.exe                    1916   1472      8    208 2019-07-18 01
 0xfffffa80023dcb10:csrss.exe
---snip---

# vol.py -f /mnt/hgfs/Temp/memdump.mem --profile Win7SP1x64 pstree | egrep "(services.exe|sv
Volatility Foundation Volatility Framework 2.6.1
. 0xfffffa800273c7b0:services.exe                     496    396     11    237 2019-07-18 01
.. 0xfffffa8002d83b10:svchost.exe                    2092    496      5     95 2019-07-18 01
.. 0xfffffa800133b170:svchost.exe                    3716    496     13    355 2019-07-18 01
.. 0xfffffa8002846900:svchost.exe                     804    496     21    464 2019-07-18 01
.. 0xfffffa8002920870:svchost.exe                     296    496     19    506 2019-07-18 01
.. 0xfffffa8002aa9b10:svchost.exe                    1408    496     11    315 2019-07-18 01
.. 0xfffffa80028909c0:svchost.exe                     868    496     20    623 2019-07-18 01
.. 0xfffffa8002ad6060:svchost.exe                    1480    496      8    176 2019-07-18 01
.. 0xfffffa8002888b10:svchost.exe                     844    496     18    393 2019-07-18 01
.. 0xfffffa8002815550:svchost.exe                     720    496      9    284 2019-07-18 01
.. 0xfffffa80028df6a0:svchost.exe                     988    496      7    123 2019-07-18 01
.. 0xfffffa80027c1060:svchost.exe                     616    496     11    366 2019-07-18 01
.. 0xfffffa8002995b10:svchost.exe                    1140    496     19    328 2019-07-18 01
.. 0xfffffa80028aeb10:svchost.exe                     916    496     36    934 2019-07-18 01
. 0xfffffa800309e6c0:svchost.exe                     2152   1472      8     82 2019-07-18 01
```

What is the origin/absolute file path from which the malicious has been started?
`C:\Users\IEUser\Downloads\YoutTube_Downloader_Free\svchost.exe`

```
# vol.py -f /mnt/hgfs/Temp/memdump.mem --profile Win7SP1x64 filescan | grep "IEUser" | grep "
Volatility Foundation Volatility Framework 2.6.1
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
---snip---
0x000000003f9864d0      3      0 R--r-d \Device\HarddiskVolume1\Users\IEUser\Downloads\YoutTu
---snip---
```

The monitoring system has set of an alarm due to a detected executable file inside an archive file. Where has it been downloaded from?

- Direct link: http://download1646.mediafire.com/s4arsed52mtg/ggczopkdtj7e96k/YoutTube_Downloader_
- Landing page: http://www.mediafire.com/file/ggczopkdtj7e96k/YoutTube_Downloader_Free.zip/file
- Under Wireshark File->Export Objects-> HTTP… Packet 84926 has the content type application/zip. This can be found easily by using the sort functionality of the Size column header. Click on the entry and the packet will be selected in Wireshark
- Right click -> Follow -> HTTP Stream
- The HTTP-Header Referer shows from which site the download of the zip file has been initiated (landing page)
- Merging the host header and the requested paths leads to the direct link.

```
GET /jyjp9xyluamg/ggczopkdtj7e96k/YoutTube_Downloader_Free.zip HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.mediafire.com/file/ggczopkdtj7e96k/YoutTube_Downloader_Free.zip/file
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: download1646.mediafire.com
DNT: 1
Connection: Keep-Alive
Cookie: __cfduid=d6c39f003771226b40939716f9e470e241563376311; ukey=2yn8lgnyuhcmfs6qrp4oxrdwg

HTTP/1.1 200 OK
Server: LRBD-ab58398
Date: Wed, 17 Jul 2019 15:12:15 GMT
Connection: close
Accept-Ranges: bytes
Content-transfer-encoding: binary
Content-Length: 3075730
```

```
Cache-Control: no-store
X-Robots-Tag: noindex, nofollow
Content-Disposition: attachment; filename="YoutTube_Downloader_Free.zip"
Content-Type: application/zip

PK
```

Investigate the traffic and provide the SHA256 hashes of suspected malicious files. Explain what likely might have happened.

- Download of YoutTube_Downloader_Free.zip from Mediafire
- Execution of extracted svchost.exe from the archive

```
# sha256sum YoutTube_Downloader_Free.zip
11c42e4fa2db0aa5f19125a5522fa961d8bc63b3385c1e3fbcbf40a52f873a89  YoutTube_Downloader_Free.zi

# sha256sum svchost.exe
20d1a2eedd7053f9fdb22c2365079a21e7d475b806bd5db519ef18172d637b0e  svchost.exe
```

Are there any suspicious network connections visible in the memory dump? If yes, provide thel local address and port as well as the foreign address and port and the state of the connection. Inspect the traffic to find suspicious connections.

- The traffic log shows suspicious DNS requests after the Zip file has been downloaded.
- The address 51.15.43.110 has to be checked in the memory dump.
- The local address and port is 192.168.17.225:59944.
- The remote address and port is 51.15.43.110:443.
- The state of the connection is established.

```
# Wireshark (Traffic) Output
85062   179.143092  192.168.17.225  192.168.17.1    DNS 90  Standard query 0x6861 A merlin.ic
85063   179.216258  192.168.17.1    192.168.17.225  DNS 106 Standard query response 0x6861 A
```

```
# Volatility (Memory Dump) Output
# vol.py -f /mnt/hgfs/Temp/memdump.mem --profile Win7SP1x64 netscan | grep "51.15.43.110"
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State
0x3fa8b730         TCPv4    192.168.17.225:59944           51.15.43.110:443     ESTABLISHED
```

Are the any indicators of stolen data?

- Checking the Statistics -> Conversations -> IPv4 feature, sort for Bytes B->A column header. After sorting the transfer of 4,555 kB from the investigated system to the IP 51.15.43.110 are visible and indicating data exfiltration/theft.