



HARARE INSTITUTE OF TECHNOLOGY

INFORMATION SECURITY AND ASSURANCE PART

4

ISHEANESU MAGAYA H140170G

COMPUTER FORENSICS LAB One – Windows Live
Response

TUTOR: MR MARENGEREKE

Task 1 Creating a file volatile_1_03_2016.txt	
TOOLS REQUIRED TO PERFORM TASK: cmd.exe	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
NO ARGUMENTS FOUND	
Filename	Name of the file to be created
Length	Size of the file to be created

SCREENSHOTS

```
C:\Users\user>cd C:\Users\user\Documents\4.2\LABS\Forencics
C:\Users\user\Documents\4.2\LABS\Forencics>fsutil file createnew volatile_26_02_2018.txt 0
File C:\Users\user\Documents\4.2\LABS\Forencics\volatile_26_02_2018.txt is created
```

COMMAND: fsutil file createnew volatile_26_02_2018.txt 0

It will create an empty file named volatile_26_02_2018.txt 0

Task 2 Find the md5 of the text file volatile_1_03_2016.txt	
TOOLS REQUIRED TO PERFORM TASK: md5sum	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-b	Read the file in binary mode
-c	Check md5sums against a given list
--status	Don't output anything, status code shows success
-w	Warn about improperly formatted md5sum checksum files
--help	Displays help text
--version	Output the version information and exit

SCREENSHOTS

```
C:\Users\user\Documents\4.2\LABS\Forencics>md5sum volatile_26_02_2018.txt >>volatile_checksum.txt
C:\Users\user\Documents\4.2\LABS\Forencics>md5sum.exe volatile_26_02_2018.txt
d41d8cd98f00b204e9800998ecf8427e *volatile_26_02_2018.txt
```

COMMAND: md5sum volatile_26_02_2018.txt >>volatile_checksum.txt

Creates an md5 of the file volatile_26_02_2018.txt and stores it in the file volatile_checksum.txt

Task 3: Find the system date	
TOOLS REQUIRED TO PERFORM TASK : date.exe	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
/t	switch which tells the command to just output the current date, without prompting for a new date.

SCREENSHOTS

```
C:\Users\user\Documents\4.2\LABS\Forencics>date /t >> volatile_26_02_2018.txt
C:\Users\user\Documents\4.2\LABS\Forencics>time /t >> volatile_26_02_2018.txt
```

COMMAND: date /t >> volatile_26_02_2018.txt

Gets the system date and stores it in the text file volatile_26_02_2018.txt

Task 4: Find the system time	
TOOLS REQUIRED TO PERFORM TASK : date.exe	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
/t	Switch which tells the command to just output the current date, without prompting for a new time.

SCREENSHOT

```
C:\Users\user\Documents\4.2\LABS\Forencics>date /t >> volatile_26_02_2018.txt
C:\Users\user\Documents\4.2\LABS\Forencics>time /t >> volatile_26_02_2018.txt
```

COMMAND: time /t >> volatile_26_02_2018.txt

Gets the system time and stores it in the text file volatile_26_02_2018.txt

Task 5: Find current network connections	
TOOLS REQUIRED TO PERFORM TASK : netstat	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port
-e	Displays Ethernet statistics
-f	Displays the Fully Qualified Domain Name for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID that is associated with each connection
-p proto	Shows the connections for the protocols specified by proto
-q	Displays all connections listening ports and bound all non-listening ports.
-r	Displays the non-listening ports
-s	Displays per protocol statistics
-t	Displays current connection offload state
-x	Displays network direct connections, listeners and shared endpoints
-y	Displays the TCP connection template for all the connections.
-interval	Displays selected statistics, pausing interval seconds between each display.

```

Microsoft Windows [Version 10.0.17093.1000]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>netstat -an

Active Connections

  Proto Local Address           Foreign Address         State
  TCP    0.0.0.0:22               0.0.0.0:0               LISTENING
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:623              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:902              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:912              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1536             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1537             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1538             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1539             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1540             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1541             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1542             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:1560             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:2291             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:2701             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:2869             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:3389             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:3790             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:5432             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:5700             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:7680             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:8884             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:9012             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:10617            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:16992            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:50080            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:50443            0.0.0.0:0               LISTENING
  TCP    10.9.143.127:139         0.0.0.0:0               LISTENING
  TCP    10.9.143.127:1734        13.107.3.128:443        CLOSE_WAIT
  TCP    10.9.143.127:1806        41.60.207.14:443        ESTABLISHED
  TCP    10.9.143.127:2056        131.253.61.100:443      TIME_WAIT
  TCP    10.9.143.127:2057        40.127.129.109:443      TIME_WAIT
  TCP    10.9.143.127:2058        40.127.129.109:443      TIME_WAIT
  TCP    10.9.143.127:2061        144.76.8.69:8333        SYN_SENT
  TCP    10.9.143.127:2063        40.127.129.109:443      TIME_WAIT
  TCP    10.9.143.127:2071        40.127.129.109:443      TIME_WAIT

```

SCREENSHOTS

COMMAND: netstat -an Displays all the connections and listening ports

Task 6: Determining which executable are opening TCP or UDP Ports

TOOLS REQUIRED TO PERFORM TASK: netstat	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port
-e	Displays Ethernet statistics
-f	Displays the Fully Qualified Domain Name for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID that is associated with each connection
-p proto	Shows the connections for the protocols specified by proto.
-q	Displays all connections listening ports and bound all non-listening ports.
-r	Displays the non-listening ports
-s	Displays per protocol statistics
-t	Displays current connection offload state
-x	Displays network direct connections, listeners and shared endpoints
-y	Displays the TCP connection template for all the connections.
-interval	Displays selected statistics, pausing interval seconds between each display.

Screen Shot

```
C:\Users\user\Documents\4.2\LABS\Forencics>netstat -anp udp>>volatile_26_02_2018.txt
```

Command: netstat -anp udp>>filename

Task 7: Find the Internal Routing Table	
TOOLS USED TO PERFORM TASK: netstat -rn	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port
-e	Displays Ethernet statistics
-f	Displays the Fully Qualified Domain Name for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID that is associated with each connection
-p proto	Shows the connections for the protocols specified by proto.
-q	Displays all connections listening ports and bound all non-listening ports.
-r	Displays the non-listening ports
-s	Displays per protocol statistics
-t	Displays current connection offload state
-x	Displays network direct connections, listeners and shared endpoints
-y	Displays the TCP connection template for all the connections.
-interval	Displays selected statistics, pausing interval seconds between each display.

SCREENSHOTS


```

C:\Users\user\Documents\4.2\LABS\Forencics>netstat -rn
=====
Interface List
17...f8 ca b8 52 3e 5f .....Intel(R) Ethernet Connection (3) I218-LM
27...10 02 b5 2e 3d 9a .....Microsoft Wi-Fi Direct Virtual Adapter #2
16...12 02 b5 2e 3d 99 .....Microsoft Wi-Fi Direct Virtual Adapter #3
12...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
14...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
4...00 ff 24 75 5b b9 .....TAP-Windows Adapter V9
9...c6 dc cb 62 79 dd .....Intel(R) Dual Band Wireless-AC 7265
19...10 02 b5 2e 3d 9d .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.9.0.1         10.9.143.127     55
10.9.0.0                    255.255.0.0      On-link          10.9.143.127     311
10.9.143.127                255.255.255.255  On-link          10.9.143.127     311
10.9.255.255                255.255.255.255  On-link          10.9.143.127     311
127.0.0.0                    255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                    255.255.255.255  On-link          127.0.0.1        331
127.255.255.255             255.255.255.255  On-link          127.0.0.1        331
192.168.42.0                 255.255.255.0    On-link          192.168.42.1     291
192.168.42.1                 255.255.255.255  On-link          192.168.42.1     291
192.168.42.255               255.255.255.255  On-link          192.168.42.1     291
192.168.159.0                255.255.255.0    On-link          192.168.159.1    291
192.168.159.1                255.255.255.255  On-link          192.168.159.1    291
192.168.159.255              255.255.255.255  On-link          192.168.159.1    291
224.0.0.0                    240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                    240.0.0.0        On-link          10.9.143.127     311
224.0.0.0                    240.0.0.0        On-link          192.168.42.1     291
224.0.0.0                    240.0.0.0        On-link          192.168.159.1    291
255.255.255.255              255.255.255.255  On-link          127.0.0.1        331
255.255.255.255              255.255.255.255  On-link          10.9.143.127     311
255.255.255.255              255.255.255.255  On-link          192.168.42.1     291
255.255.255.255              255.255.255.255  On-link          192.168.159.1    291
=====
Persistent Routes:
None

```

```

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination Gateway
1 331 ::1/128 On-link
9 311 fe80::/64 On-link
14 291 fe80::/64 On-link
12 291 fe80::/64 On-link
12 291 fe80::4192:f188:2150:5b8b/128 On-link
14 291 fe80::6403:45ba:cc37:e03f/128 On-link
9 311 fe80::9558:e09b:b4cd:cc3f/128 On-link
1 331 ff00::/8 On-link
9 311 ff00::/8 On-link
14 291 ff00::/8 On-link
12 291 ff00::/8 On-link
=====
Persistent Routes:
None

```

Command used: netstat -rn. Displays the internal routing table

Task 8: Determining open TCP connections	
TOOLS USED TO PERFORM TASK: netstat -anp tcp	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port
-e	Displays Ethernet statistics
-f	Displays the Fully Qualified Domain Name for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID that is associated with each connection
-p proto	Shows the connections for the protocols specified by proto.
-q	Displays all connections listening ports and bound all non-listening ports.
-r	Displays the non-listening ports
-s	Displays per protocol statistics
-t	Displays current connection offload state
-x	Displays network direct connections, listeners and shared endpoints
-y	Displays the TCP connection template for all the connections
-interval	Displays selected statistics, pausing interval seconds between each display.

Screenshot

```
C:\Users\user\Documents\4.2\LABS\Forencics>netstat -anp tcp>>volatile_26_02_2018.txt
```

Command: netstat -anp TCP

Task 9: Determining which services are opening UDP connections	
TOOLS USED TO PERFORM TASK: netstat -anp udp	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port
-e	Displays Ethernet statistics
-f	Displays the Fully Qualified Domain Name for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID that is associated with each connection
-p proto	Shows the connections for the protocols specified by protocol.
-q	Displays all connections listening ports and bound all non-listening ports.
-r	Displays the non-listening ports
-s	Displays per protocol statistics
-t	Displays current connection offload state
-x	Displays network direct connections, listeners and shared endpoints
-y	Displays the UDP connection template for all the connections
-interval	Displays selected statistics, pausing interval seconds between each display.

Screen Shot

```
C:\Users\user\Documents\4.2\LABS\Forencics>netstat -anp UDP
```

Active Connections

Proto	Local Address	Foreign Address	State
UDP	0.0.0.0:123	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:3389	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:54770	*:*	
UDP	0.0.0.0:57927	*:*	
UDP	10.9.143.127:137	*:*	
UDP	10.9.143.127:138	*:*	
UDP	10.9.143.127:1900	*:*	
UDP	10.9.143.127:54886	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:29821	*:*	
UDP	127.0.0.1:54887	*:*	
UDP	127.0.0.1:59815	*:*	

Command: netstat -anp UDP

Task 10: Running Processes	
TOOLS USED TO PERFORM TASK: pslist	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-d	Show thread detail
-m	Show memory detail
-x	Show process, memory information and threads
-t	Show process tree
-s [n]	Run in task manager for the optional seconds specified
-r n	Task Manager refresh rate in seconds
\\computer	Specifies remote computer
-u	Optional username for remote login
-p	Optional password for remote login. if you don't request for it on the command line pslist may request one if necessary
-name	Show information about the process that begin with the name specified
-e	Exact name process zone
pid	Show information about the specified system

SCREENSHOTS

```
C:\Users\user\Documents\4.2\LABS\Forencics>pslist
```

```
pslist v1.28 - Sysinternals PsList  
Copyright - 2000-2004 Mark Russinovich  
Sysinternals
```

```
Process information for REDPAROLL-7THZ0:
```

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	4	0	52	43:01:04.312	46:02:25.747
System	4	8	174	8219	216	26:38:41.406	46:02:25.747
Registry	96	8	3	0	2776	0:00:09.156	46:02:47.910
smss	428	11	2	52	500	0:00:00.359	46:02:25.744
csrss	592	13	12	1087	1920	0:00:12.000	46:02:03.481
wininit	684	13	2	151	1388	0:00:00.093	46:02:03.170
services	760	9	11	1012	7920	0:20:18.500	46:02:03.114
lsass	776	9	18	2271	16608	0:02:37.968	46:02:03.099
svchost	900	8	2	84	1048	0:00:00.218	46:02:02.615
svchost	924	8	29	2892	20464	0:02:09.640	46:02:02.591
fontdrvhost	952	8	5	45	1744	0:00:00.093	46:02:02.570
svchost	388	8	20	1738	16828	0:06:11.515	46:02:02.233
svchost	552	8	11	378	3824	0:00:19.468	46:02:02.209
svchost	1188	8	32	566	5068	0:00:06.281	46:02:01.822
svchost	1244	8	7	176	7856	0:00:26.921	46:02:01.810
svchost	1268	8	4	198	1992	0:00:01.031	46:02:01.805
svchost	1324	8	8	259	2984	0:00:03.046	46:02:01.790
svchost	1400	8	4	188	2012	0:00:01.843	46:02:01.771
svchost	1448	8	10	230	2996	0:01:13.718	46:02:01.754
svchost	1468	8	4	197	2440	0:00:01.703	46:02:01.743
svchost	1560	8	17	271	6496	0:28:53.390	46:02:01.712
svchost	1568	8	14	430	6928	0:00:08.296	46:02:01.710
svchost	1708	8	3	171	1888	0:00:00.640	46:02:01.638
svchost	1796	8	4	177	1908	0:00:00.828	46:02:01.609
svchost	1864	8	7	229	2824	0:00:04.265	46:02:01.575
svchost	1892	8	16	560	19940	0:01:16.265	46:02:01.561
svchost	1396	8	3	242	2840	0:00:00.609	46:02:01.497
svchost	2056	8	3	156	2180	0:00:01.656	46:02:01.485
svchost	2112	8	5	170	2236	0:00:07.515	46:02:01.454
svchost	2148	8	8	218	2088	0:00:00.468	46:02:01.434
WUDFHost	2324	13	14	341	25152	0:00:01.484	46:02:01.306
dasHost	2336	8	4	217	3832	0:00:03.062	46:02:01.299
svchost	2344	8	10	496	19824	0:02:37.468	46:02:01.299
svchost	2364	8	7	253	4368	0:01:23.671	46:02:01.292
svchost	2444	8	6	199	2368	0:00:03.234	46:02:01.276
svchost	2508	8	9	239	118020	0:33:36.453	46:02:01.242
svchost	2516	8	5	183	2112	0:00:01.187	46:02:01.241

Command used: pslist. It lists the current processes running.

Task 11: Running Services	
TOOLS TO PERFORM TASK: psservice	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
Query	Queries the status of a service
Config	Queries the configuration
Setconfig	Sets a configuration
Start	Starts a service
Stop	Stops a service
Restart	Stops and restarts a service
Pause	Pause a service
Continue	Continue a service
Depend	Enumerates the services that depend on the one specified
find	Searches for an instance of a service on the network
security	Reports the security permissions assigned to a service

SCREENSHOTS

```
C:\Users\user\Documents\4.2\LABS\Forencics>psservice

PsService v2.21 - Service information and configuration utility
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AdobeUpdateService
DISPLAY_NAME: AdobeUpdateService
(null)
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                           (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: AGSService
DISPLAY_NAME: Adobe Genuine Software Integrity Service
Adobe Genuine Software Integrity Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                           (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1   STOPPED
                           (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
                           (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
```

Command Used: psservice. It gives the list of services that are currently running

Task 12: Find Scheduled Jobs	
TOOLS USED TO PERFORM TASK: schtasks.exe	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
NO OPTIONAL ARGUMENTS FOUND	
/Create	Creates a new scheduled task.
/Delete	Deletes the scheduled task(s).
/ShowSid	Shows the security identifier corresponding to a scheduled task name.
/End	Stops the currently running scheduled task.
/Run	Runs the scheduled task on demand.
/Change	Changes the properties of scheduled task
/Query	Displays all scheduled tasks.

SCREENSHOTS


```

C:\Users\user\Documents\4.2\LABS\Forencics>schtasks

Folder: \
TaskName                                     Next Run Time                               Status
=====
AdobeGCInvoker-1.0-MicrosoftAccount-itee  22/03/2018  7:27:00 AM  Ready
Dell SupportAssistAgent AutoUpdate         21/03/2018  8:16:08 PM  Ready
DriverPack Notifier                       21/03/2018  8:37:00 PM  Ready
Git for Windows Updater                   22/03/2018  8:32:52 AM  Ready
OneDrive Standalone Update Task-S-1-5-21  22/03/2018  8:21:29 AM  Ready
Pcd.DriverScan.7GN0K                      N/A                                             Ready
PCDDDataUploadTask                       28/03/2018  5:25:34 AM  Ready
PCDEventLauncherTask                     N/A                                             Ready
PCDoctorBackgroundMonitorTask             06/04/2018  12:00:00 AM  Ready
SystemToolsDailyTest                     21/03/2018  2:43:00 PM  Running
UCBrowserUpdater                          21/03/2018  10:58:00 AM  Ready
UCBrowserUpdaterCore                     N/A                                             Ready
User_Feed_Synchronization-{070525A5-9DE8  21/03/2018  12:39:59 PM  Ready
{911969D5-F6D1-4452-918F-F12276678FB1}  N/A                                             Ready
{BBEE1151-AD1D-4725-9DBD-48AB0AB8AE4C}  N/A                                             Ready

Folder: \Microsoft
TaskName                                     Next Run Time                               Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Configuration Manager
TaskName                                     Next Run Time                               Status
=====
Configuration Manager Health Evaluation    N/A                                             Ready

Folder: \Microsoft\Office
TaskName                                     Next Run Time                               Status
=====
Office 15 Subscription Heartbeat          22/03/2018  5:51:27 AM  Ready
OfficeTelemetryAgentFallBack2016         N/A                                             Ready
OfficeTelemetryAgentLogOn2016            N/A                                             Ready

Folder: \Microsoft\Windows
TaskName                                     Next Run Time                               Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\.NET Framework
TaskName                                     Next Run Time                               Status
=====

```

Command used: schtasks.

It gives the list of tasks that are scheduled to run

Task 13: Process Image Dumps	
TOOLS TO BE USED: userdump	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-p	Displays a list of running process and process Id's
-k	Optionally causes a process to be killed after being dumped
-m	Same as above, except that it dumps multiple files
-d	Specifies the directory to dump the files
-g	Same as above, except that it dumps win32 gui apps that appear to hang

SCREENSHOTS

```

C:\WINDOWS\system32\cmd.exe
C:\IRTOOLKIT_MUSARA\userdump>userdump /p
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights reserved.

  0 System Idle Process
  4 System
432 smss.exe
584 csrss.exe
648 csrss.exe
672 wininit.exe
728 winlogon.exe
780 services.exe
796 lsass.exe
876 svchost.exe
956 svchost.exe
 76 dwm.exe
776 svchost.exe
1088 svchost.exe
1096 svchost.exe
1128 svchost.exe
1208 svchost.exe
1272 svchost.exe
1448 svchost.exe
1924 spoolsv.exe

```

Command Used: userdump /p. displays a list of running processes and process ID's

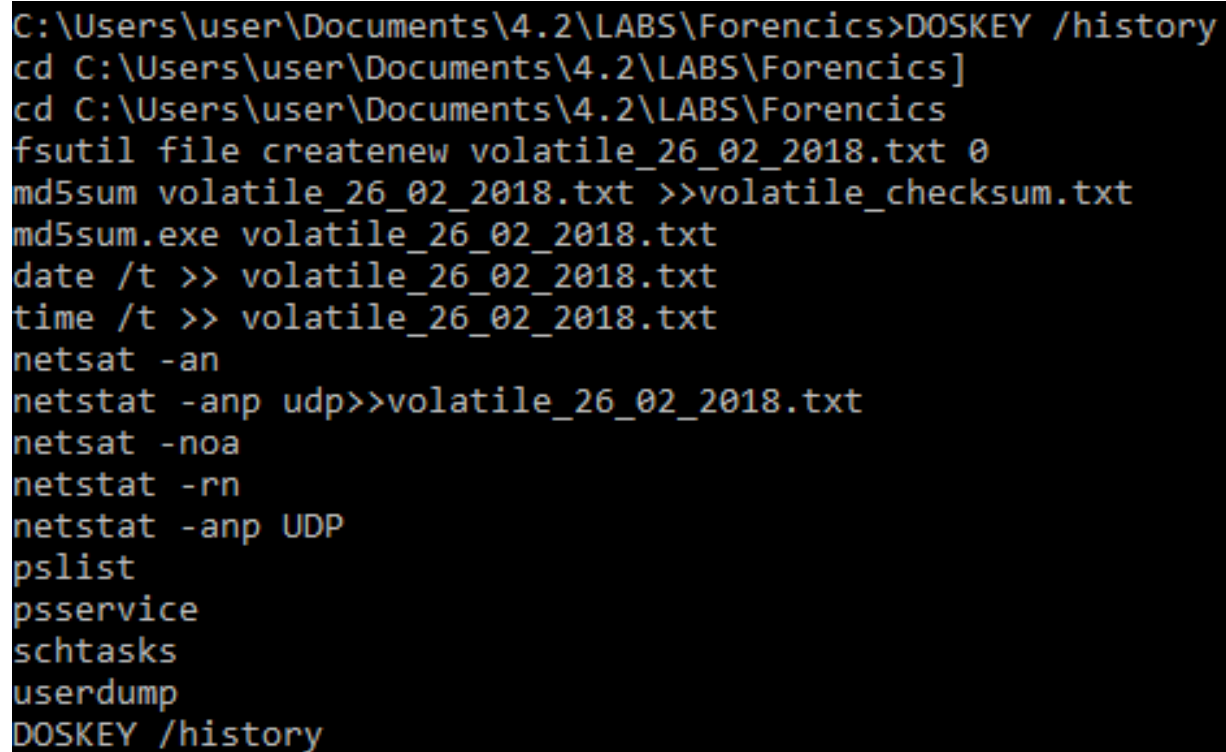
Task14: Find the History of all commands Executed

TOOLS TO BE USED: cmd.exe

LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND
--

NO OPTIONAL ARGUMENTS FOUND

SCREENSHOTS



```
C:\Users\user\Documents\4.2\LABS\Forencics>DOSKEY /history
cd C:\Users\user\Documents\4.2\LABS\Forencics]
cd C:\Users\user\Documents\4.2\LABS\Forencics
fsutil file createnew volatile_26_02_2018.txt 0
md5sum volatile_26_02_2018.txt >>volatile_checksum.txt
md5sum.exe volatile_26_02_2018.txt
date /t >> volatile_26_02_2018.txt
time /t >> volatile_26_02_2018.txt
netsat -an
netstat -anp udp>>volatile_26_02_2018.txt
netsat -noa
netstat -rn
netstat -anp UDP
pslist
psservice
schtasks
userdump
DOSKEY /history
```

Command Used: DOSKEY /history. Lists the history of all the commands performed
--

Task 15: OPEN FILES	
TOOLS TO PERFORM TASK: psfile	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-u	Specifies optional user name for login to remote computer
-p	Specifies password for user name.
Id	Id of file to print information for or close
Path	Full or partial path of files to match.
-c	Closes file identified by file Id.

Screen Shot

```
C:\Users\user\Documents\4.2\LABS\Forencics>psfile.exe

psfile v1.02 - psfile
Copyright - 2001 Mark Russinovich
Sysinternals

Error listing remotely open files on REDPAROLL-7THZO:
Access is denied.

C:\Users\user\Documents\4.2\LABS\Forencics>
```

```
C:\Users\user\Documents\4.2\LABS\Forencics>psfile.exe

psfile v1.02 - psfile
Copyright - 2001 Mark Russinovich
Sysinternals

No files opened remotely on REDPAROLL-7THZO.
```

Command : psfile.exe

Task 16: Users currently logged on	
TOOLS TO PERFORM TASK: psloggedon	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-l	Show only local logons
-x	Don't show logon times

Screen Shot

```
C:\Users\user\Documents\4.2\LABS\Forencics>PSloggedon.exe

loggedon v1.33 - See who's logged on
Copyright - 2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
    Error: could not retrieve logon time
NT AUTHORITY\LOCAL SERVICE
    Error: could not retrieve logon time
NT AUTHORITY\NETWORK SERVICE
    20/03/2018 6:08:18 AM    REDPAROLL-7THZO\user
    Error: could not retrieve logon time
NT AUTHORITY\SYSTEM

No one is logged on via resource shares.
```

Command : PSloggedon.exe

Task17: Cached NetBIOS Name Table	
TOOLS REQUIRED TO PERFORM TASK: nbtstat	
LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND	
-a	Lists the remote machine's name table given its name
-c	Lists NBT's cache of remote [machine] names and their IP addresses
-n	Lists local NetBIOS names
-r	Lists names resolved by broadcast and via WINS
-R	Purges and reloads the remote cache name table
-S	Lists sessions table with the destination IP addresses
-s	Lists sessions table converting destination IP
-A	Lists the remote machine's name table given its IP address.
-RR	Sends Name Release packets to WINS and then, starts Refresh

Screen shot

```
C:\Users\user\Documents\4.2\LABS\Forencics>nbtstat -c
```

```
VMware Network Adapter VMnet8:
```

```
Node IpAddress: [192.168.42.1] Scope Id: []
```

```
    No names in cache
```

```
VMware Network Adapter VMnet1:
```

```
Node IpAddress: [192.168.159.1] Scope Id: []
```

```
    No names in cache
```

```
Ethernet 4:
```

```
Node IpAddress: [0.0.0.0] Scope Id: []
```

```
    No names in cache
```

```
Ethernet:
```

```
Node IpAddress: [0.0.0.0] Scope Id: []
```

```
    No names in cache
```

```
Bluetooth Network Connection:
```

```
Node IpAddress: [0.0.0.0] Scope Id: []
```

```
    No names in cache
```

```
Wi-Fi:
```

```
Node IpAddress: [0.0.0.0] Scope Id: []
```

```
    No names in cache
```

```
Local Area Connection* 3:
```

```
Node IpAddress: [0.0.0.0] Scope Id: []
```

```
    No names in cache
```

```
Local Area Connection* 4:
```

```
Node IpAddress: [192.168.137.1] Scope Id: []
```

```
    No names in cache
```

```
Ethernet 8:
```

```
Node IpAddress: [192.168.42.35] Scope Id: []
```

COMMAND: nbtstat -c> > volatile_26_02_2018.txt

Task17: Calculate the second md5 of volatile_1_03_2016.txt

TOOLS REQUIRED TO PERFORM TASK: md5sum

LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND

-b	Read the file in binary mode
-c	Check md5sums against a given list
--status	Don't output anything, status code shows success
-w	Warn about improperly formatted md5sum checksum files
--help	Displays help text
--version	Output the version information and exit

SCREENSHOTS

```
C:\Users\user\Documents\4.2\LABS\Forencics>md5sum volatile_26_02_2018.txt >> volatile_26_02_2018.txt
```

COMMAND: md5sum volatile_26_02_2018.txt >> volatile_26_02_2018.txt

Creates an md5 of the file volatile_26_02_2018.txt and stores it in the file in the file volatile_26_02_2018.txt