EX NO : 5 **File forensics**

Investigating MS Word documents

1) Note: DOCX is the file format for Microsoft Office 2007 and later. DOCX should not be confused with DOC, the format used by earlier versions of Microsoft Office.

It is possible to say something about the revision history of MS Word documents using forensic tools.

a) The Strings utility is available from the following Web site

https://docs.microsoft.com/en-us/sysinternals/downloads/strings
Strings just scans the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters

b) DCode is a forensic tool (currently available free) at the following Web site:

https://www.digital-detective.net/dcode/
Use these tools to see if you can say something about the revision history of MS Word documents.

2) Have you ever tried to open a Word Docx file in notepad? If so, then you know that you get a screen full of unintelligible characters. All you need to do is run the Docx file through an unzip program and you can see several files and folders full of XML data. The files can now be opened in Notepad, but if you just double click on them, they will open in your Web browser and be a bit more readable. Browse through the newly created folders and you will find plenty of formatting information and the complete text of the document. You will also find information that could be very useful for forensics. Including files revision, creation and modify dates, document creator and who was the last one to modify the document.

Investigate doc and docx files and include screenshots in your submission

Aim :

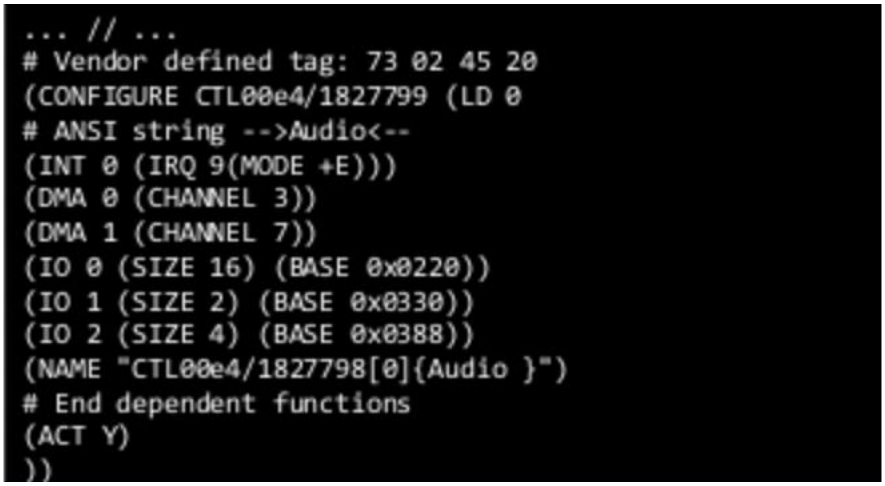
To perform forensic investigation of files such as Microsoft Word documents

Algorithm / Procedure:
Make use of the utilities such as Strings and the DCode tool.

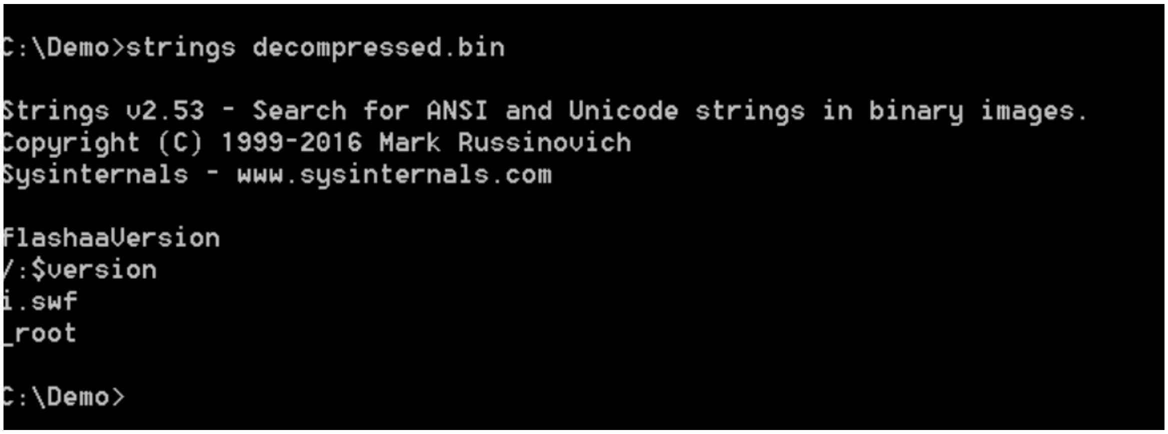
Sample Coding : The utilities are used. No coding involved.

Sample Input : See the screenshots below

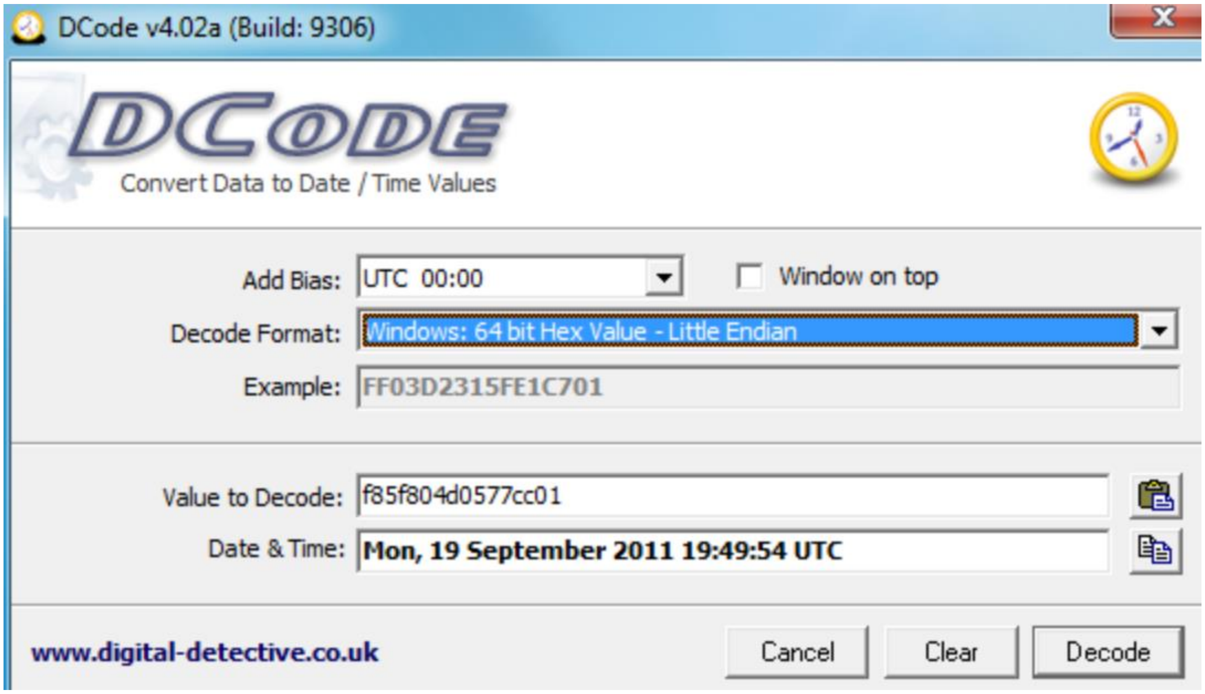
Sample Output :



```
... // ...
# Vendor defined tag: 73 02 45 20
(CONFIGURE CTL00e4/1827799 (LD 0
# ANSI string -->Audio<--
(INT 0 (IRQ 9(MODE +E)))
(DMA 0 (CHANNEL 3))
(DMA 1 (CHANNEL 7))
(IO 0 (SIZE 16) (BASE 0x0220))
(IO 1 (SIZE 2) (BASE 0x0330))
(IO 2 (SIZE 4) (BASE 0x0388))
(NAME "CTL00e4/1827798[0]{Audio }")
# End dependent functions
(ACT Y)
))
```



```
C:\Demo>strings decompressed.bin

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

FlashaaVersion
/:$version
i.swf
_root

C:\Demo>
```


DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
www.digital-detective.co.uk
Cancel
Clear
Decode

Add Bias: UTC 00:00

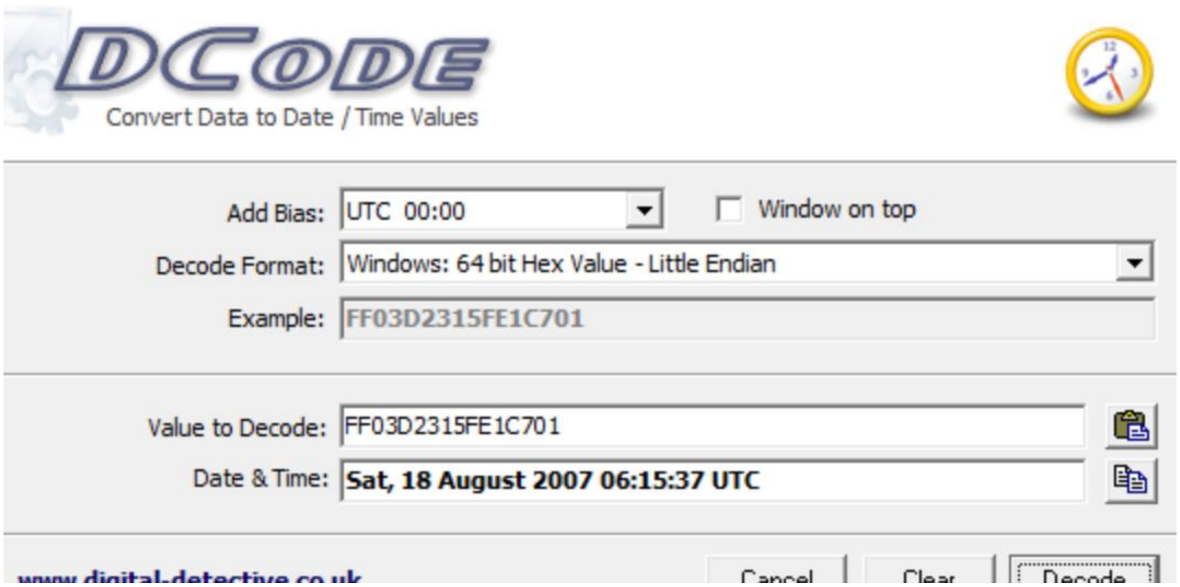
□ Window on top

Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: f85f804d0577cc01

Date & Time: Mon, 19 September 2011 19:49:54 UTC


DCODE
Convert Data to Date / Time Values
□ Window on top
www.digital-detective.co.uk
Cancel
Clear
Decode

Add Bias: UTC 00:00

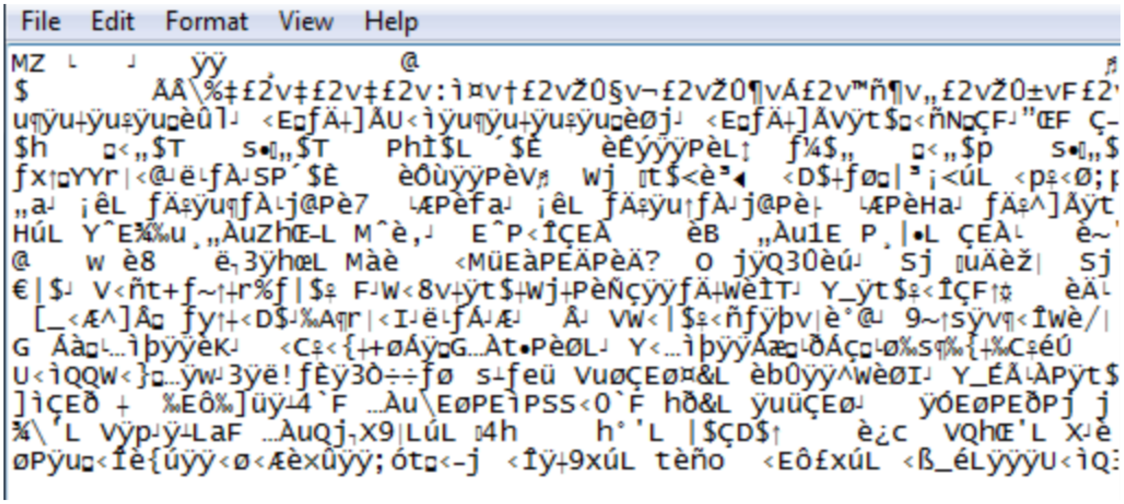
Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

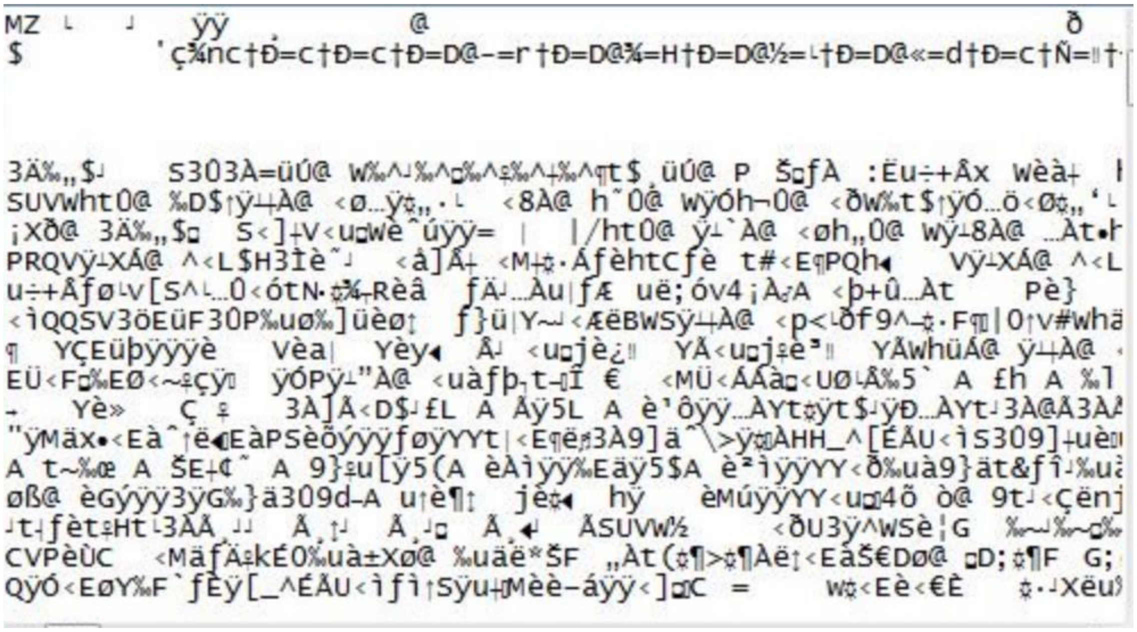
Value to Decode: FF03D2315FE1C701

Date & Time: Sat, 18 August 2007 06:15:37 UTC

Screenshot:



```
MZ └    ┘    ÿÿ  ¸          @                                          ♬
$         ÄÅ\%‡£2v‡£2v‡£2v:ì¤v†£2vŽ0§v¬£2vŽ0¶vÁ£2v™ñ¶v„£2vŽ0±vF£2
u¶ÿu┼ÿu♀ÿu◘èû1┘ <E◘fÄ┼]ÅU<ìÿu¶ÿu┼ÿu♀ÿu◘èØj┘ <E◘fÄ┼]ÅVÿt$◘<ñN◘ÇF┘"ŒF Ç-
$h    ◘<„$T    s•▯„$T    PhÌ$L ´$E    èÉýÿÿPèL↕  f¼$„    ◘<„$p    s•▯„$
fx↑◘YYr|<@┘ë└fÀ┘SP´$È    èÔùÿÿPèV♬  Wj ▯t$<è³◂  <D$┼fø◘|³¡<úL  <p♀<Ø;
„a┘ ¡êL fÄ♀ÿu¶fÀ└j@Pè7  └ÆPèfa┘ ¡êL fÄ♀ÿu↑fÀ┘j@Pè┼  └ÆPèHa┘ fÄ♀^]Åÿt
HúL Y^E¾‰u¸„ÀuZhŒ-L M^è,┘  E^P<ÎÇEÀ    èB  „Àu1E P¸|•L ÇEÀ└   è~
@   w è8   ë┐3ÿhœL Màè   <MüEàPEÄPèÄ?  O jÿQ3Ûèú┘  Sj ▯uÄèž|  Sj
€|$┘ V<ñt+f~↑┼r%f|$♀ F┘W<8v┼ÿt$┼Wj┼PèÑçÿÿfÄ┼WèÌT┘ Y_ÿt$♀<ÎÇF↑☼   èÄ└
 [_<Æ^]Å◘ fy↑┼<D$┘‰A¶r|<I┘ë└fÁ┘Æ┘  Å┘ VW<|$♀<ñfÿþv|è°@┘ 9~↑sÿv¶<Îwè/|
G Áà◘└…ìþÿÿèK┘  <C♀<{┼+øÁÿ◘G…Àt•PèØL┘ Y<…ìþÿÿÁæ◘└ðÁç◘└ø‰s¶‰{┼‰C♀éÚ
U<ìQQW<}◘…ÿw┘3ÿë!fÈÿ3ò÷÷fø s┴feü VuøÇEø¤&L èbÛÿÿ^WèØI┘ Y_ÉÅ└ÀPÿt$
]ìÇEð ┼  ‰Eô‰]üÿ┴4`F …Àu\EøPEìPSS<O`F hð&L ÿuüÇEø┘   ÿÓEøPEðPj j
¾\'L Vÿp┘ÿ┴LaF …ÀuQj┐X9|LúL ▯4h     h°'L |$ÇD$↑     è¿c  VQhŒ'L X┘è
øPÿu◘<Îè{úÿÿ<ø<Æèxûÿÿ;ót◘<-j <Îÿ┼9xúL tèño  <EÔ£xúL <ß_éLÿÿÿU<ìQ:
```



```
MZ └    ┘    ÿÿ          @                                    ð
$         'ç¾nc†Đ=c†Đ=c†Đ=D@-=r†Đ=D@¾=H†Đ=D@½=└†Đ=D@«=d†Đ=c†Ñ=‼†·


3Ä‰„$┘    S3Û3À=üÚ@ W‰^┘‰^□‰^♀‰^┼‰^¶t$ üÚ@ P Š□ƒÀ :Ëu÷+Åx Wèà┼ Ⅰ
SUVWhtÛ@ ‰D$↑ÿ┴À@ <ø…ÿ☼„·└  <8À@ h˜Û@ WÿÓh¬Û@ <ðW‰t$↑ÿÓ…ö<Ø☼„'└
¡Xð@ 3Ä‰„$□  S<]┼V<u□Wè˜úÿÿ= |  |/htÛ@ ÿ┴`À@ <øh„Û@ Wÿ┴8À@ …Àt•Ⅰ
PRQVÿ┴XÁ@ ^<L$H3Ìè˜┘  <å]Å┼ <M┼☼·ÁƒèhtCƒè t#<E¶PQh◄   Vÿ┴XÁ@ ^<L
u÷+Åƒø└v[S^└…Û<ótN·☼¾┬Rèâ  ƒÄ┘…Àu|ƒÆ uë;óv4¡À♂A <þ+û…Àt    Pè}
<ìQQSV3öEüF3ÛP‰uø‰]üèø↕  ƒ}ü|Y~┘<ÆëBWSÿ┴À@ <p<└ðf9^┴☼·F¶|0↑v#Whä
¶  YÇEüþÿÿÿè   Vèa|  Yèy◄  Å┘ <u□jè¿‼  YĂ<u□j♀è³‼  YĂWhüÁ@ ÿ┴À@ <
EÜ<F□‰EØ<~♀çÿ□  ÿÓPÿ┴"À@ <uàƒþ┐t┤□Ï €  <MÜ<ÁÁà□<UØ└Å‰5` A £h A ‰1
→   Yè»   Ç ♀   3À]Å<D$┘£L A Åÿ5L A è'ôÿÿ…ÀYt☼ÿt$┘ÿÐ…ÀYt┘3À@Å3ÀÅ
"ÿMäx•<Eà^↑ë◄EàPSèõýÿÿƒøÿYYt|<E¶ë♯3À9]ä^\>ÿ☼ÀHH_^[ÉÅU<ìS309]┼uè□
A t~‰œ A ŠE┼¢˜  A 9}♀u[ÿ5(A èÀìÿÿ‰Eäÿ5$A è²ìÿÿYY<ð‰uà9}ät&ƒî┘‰uà
øß@ èGýÿÿ3ÿG‰}ä309d–A u↑è¶↕  jè☼◄  hÿ   èMúÿÿYY<u□4õ ò@ 9t┘<Çënj
┘t┤ƒèt♀Ht└3ÀÅ ┘┘  Å ↕┘  Å ┘□  Å ◄   ÅSUVW½      <ðU3ÿ^WSè¦G  ‰~┘‰~□‰
CVPèÙC   <MäƒÄ♀kÉ0‰uà±Xø@ ‰uäë*ŠF „Àt(☼¶>☼¶Àë↕<EàŠ€Dø@ □D;☼¶F  G;
QÿÓ<EøY‰F`ƒÈÿ[_^ÉÅU<ìƒì↑Sÿu┼□Mèè–áÿÿ<]□C  =    W☼<Eè<€È   ☼·┘Xëu
```

EX NO : 6 **The Windows Command Line**

Forensics investigators should be familiar with the use of the Windows command line when they investigate computers that use the Windows operating system. Forensics software sometimes necessitates the use of the command line. Forensics recovery and data reconstruction requires an understanding of the command line syntax. Before shutting down a computer, the forensic examiner should often capture the volatile information in the system's RAM. Information such as current IP address, contents of RAM, Address Resolution Protocol (ARP) tables and current network connection status are not available once the computer has been turned off. Hence the forensic examiner must be familiar with the commands and techniques used to obtain such information on site.

Some DOS commands. Try these.

CD MD RD COPY ATTRIB DISKCOPY DATE TIME DIR PAUSE NETSTAT TYPE DEL VER DOSKEY PATH PROMPT LABEL VOL DEFRAG XCOPY ECHO REM MOVE EXIT FORMAT REN TREE MORE PRINT HELP IPCONFIG ARP CMD CALL CHCP CHKDSK CHOICE CLS ERASE DIR FC COMP FIND FOR IF MODE RECOVER SET SORT SUBST

Note: Some of the above commands are internal commands. Others are external commands. An external command is an MS-DOS command that is not included in command.com. External commands are commonly external either because they have large requirements or are not commonly used commands. Some external commands are in the above list. Some more are listed here:

BOOTSECT BCTEDIT DISKCOMP HOSTNAME ICACLS CHKNTFS NBTSTAT NET NETSH PING NSLOOKUP ROUTE PATHPING SYSTEMINFO WMIC FTP TRACERT

Exercise

1) Use commands to find the IPv4 address and subnet mask of your computer.

2) Create a batch file that will capture the following volatile information from an evidence system and store it in a file.

   Current IPv4 address
   Current date
   Current time
   ARP table
   Network connection information
   Take screenshots in both cases and include them in your submission.

   Note: The ARP (Address Resolution Protocol) cache is a collection of ARP entries (mostly dynamic) that are created when a hostname is resolved to an IP address and then an IP address is resolved to a MAC address (so the computer can effectively communicate with the IP address). ARP cache has the disadvantage of being used by hackers and cyber attackers. ARP cache helps the attackers hide behind a fake IP address and do the harm without being caught. ARP cache can also help to prevent the attacks.
   (see https://en.wikipedia.org/wiki/ARP_cache)

Aim :

To become familiar with the Windows command line for digital forensics investigations

Algorithm / Procedure:

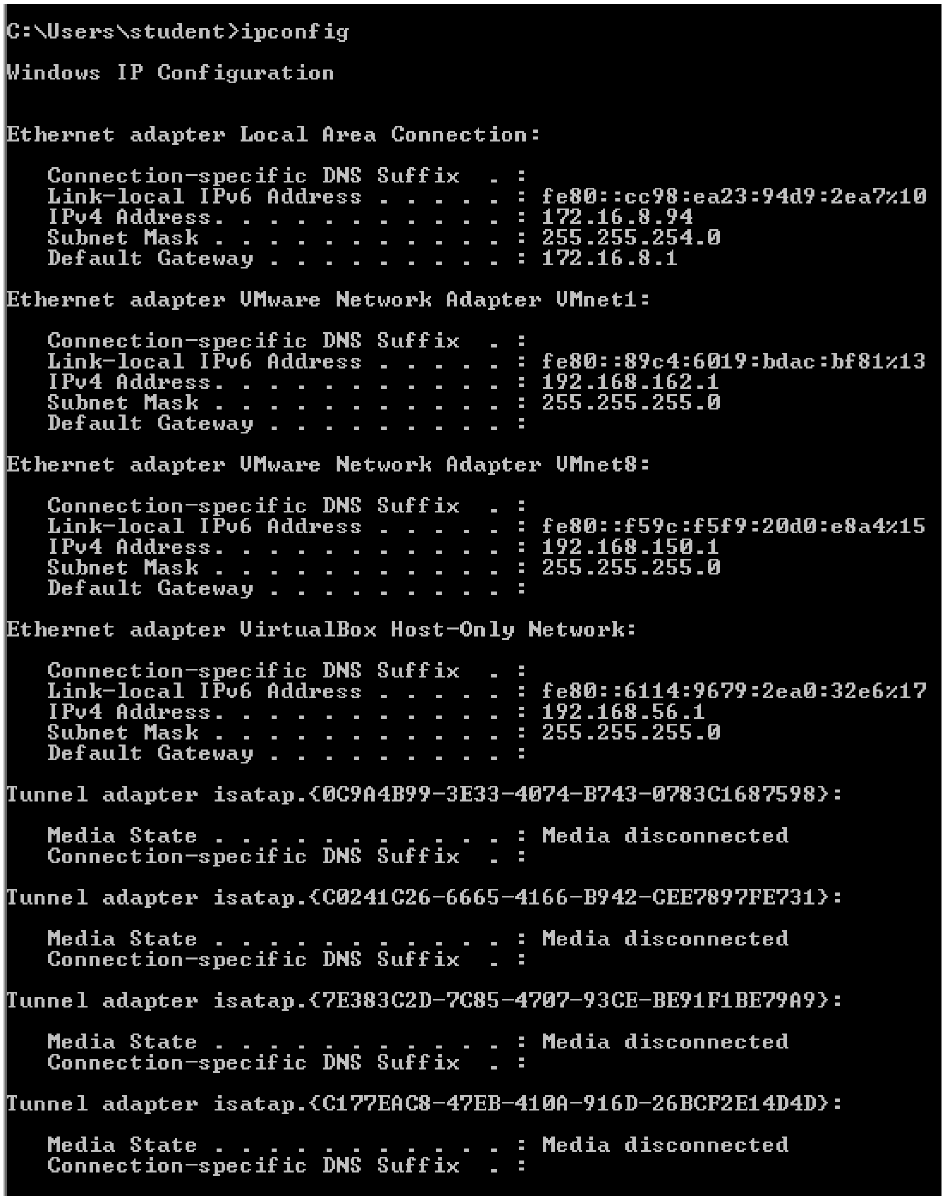
Make use of the appropriate Windows command

Sample Coding : See output

Sample Input : See screenshots below

Sample Output :

Use commands to find the IPv4 address and subnet mask of your computer. Command used is Ipconfig



```
C:\Users\student>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cc98:ea23:94d9:2ea7%10
   IPv4 Address. . . . . . . . . . . : 172.16.8.94
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.8.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::89c4:6019:bdac:bf81%13
   IPv4 Address. . . . . . . . . . . : 192.168.162.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f59c:f5f9:20d0:e8a4%15
   IPv4 Address. . . . . . . . . . . : 192.168.150.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6114:9679:2ea0:32e6%17
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{0C9A4B99-3E33-4074-B743-0783C1687598}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{C0241C26-6665-4166-B942-CEE7897FE731}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{7E383C2D-7C85-4707-93CE-BE91F1BE79A9}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{C177EAC8-47EB-410A-916D-26BCF2E14D4D}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Create a batch file that will capture the following volatile information from an evidence system and store it a file.

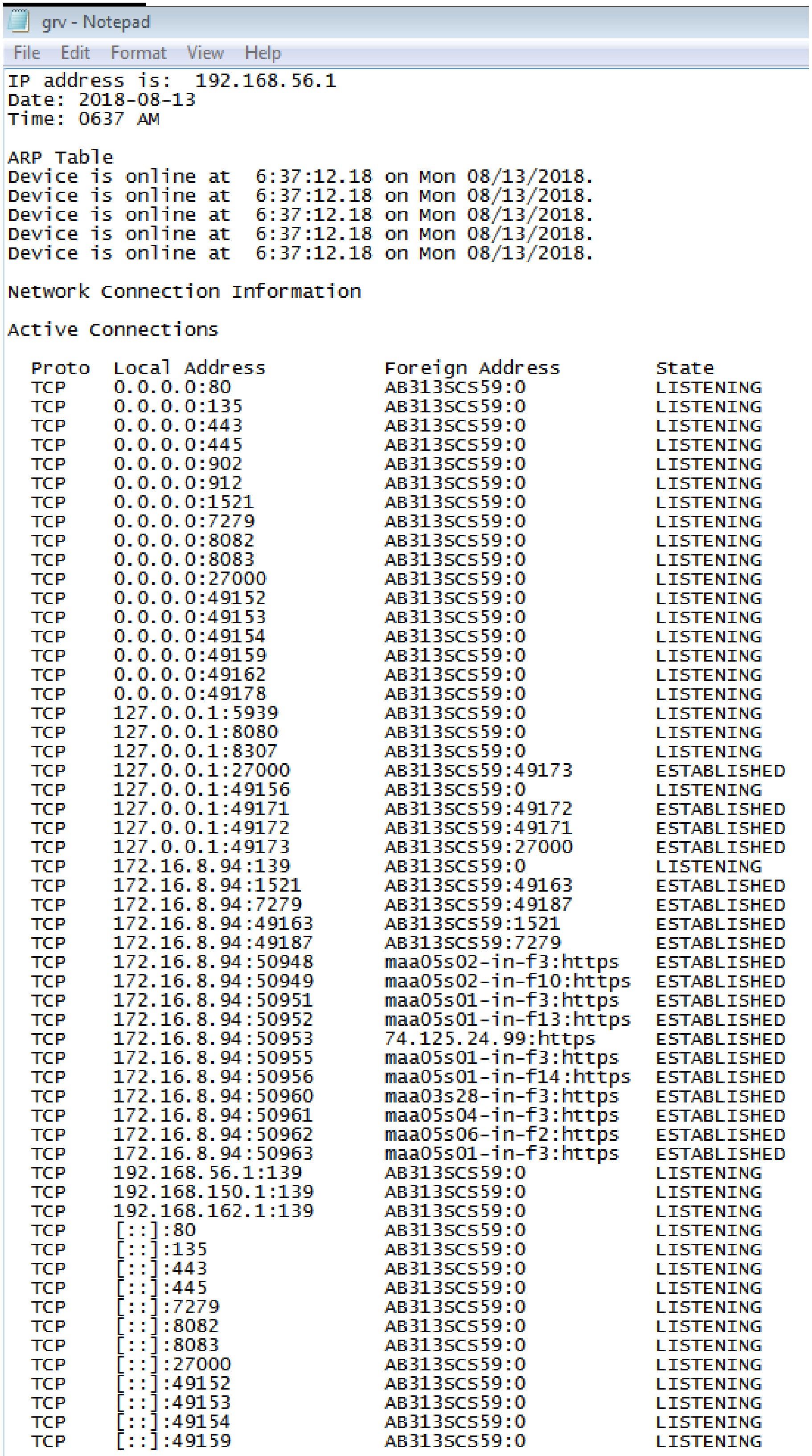
Current IPv4 address
Current date
Current time
ARP table
Network connection information

Code used:

```
@echo off
FOR /F "delims=: tokens=2" %%a in ('ipconfig ^| find "IPv4"') do set _IPAddress=%%a
```

```
ECHO IP address is: %_IPAddress% >> grv.txt

For /f "tokens=2-4 delims=/ " %%a in ('date /t') do (set mydate=%%c-%%a-%%b)
For /f "tokens=1-2 delims=/:" %%a in ('time /t') do (set mytime=%%a%%b)
echo Date: %mydate% >>grv.txt
echo Time: %mytime% >>grv.txt

echo. >>grv.txt

echo ARP Table >>grv.txt
FOR /L %%A IN (1,1,5) DO (
arp -a | findstr 20-7c-8f-3f-03-9c
cls
if %errorlevel% GEQ 1 (
echo The device is offline
Echo Device is offline at %time% on %date%. >> grv.txt
) else (
echo The device is online.
Echo Device is online at %time% on %date%. >> grv.txt
)
timeout 3 >nul /nobreak
)

echo. >>grv.txt

echo Network Connection Information >>grv.txt
netstat -a>>grv.txt
```

Screenshot:



```
IP address is:  192.168.56.1
Date: 2018-08-13
Time: 0637 AM

ARP Table
Device is online at  6:37:12.18 on Mon 08/13/2018.
Device is online at  6:37:12.18 on Mon 08/13/2018.
Device is online at  6:37:12.18 on Mon 08/13/2018.
Device is online at  6:37:12.18 on Mon 08/13/2018.
Device is online at  6:37:12.18 on Mon 08/13/2018.

Network Connection Information

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             AB313SCS59:0           LISTENING
  TCP    0.0.0.0:135            AB313SCS59:0           LISTENING
  TCP    0.0.0.0:443            AB313SCS59:0           LISTENING
  TCP    0.0.0.0:445            AB313SCS59:0           LISTENING
  TCP    0.0.0.0:902            AB313SCS59:0           LISTENING
  TCP    0.0.0.0:912            AB313SCS59:0           LISTENING
  TCP    0.0.0.0:1521           AB313SCS59:0           LISTENING
  TCP    0.0.0.0:7279           AB313SCS59:0           LISTENING
  TCP    0.0.0.0:8082           AB313SCS59:0           LISTENING
  TCP    0.0.0.0:8083           AB313SCS59:0           LISTENING
  TCP    0.0.0.0:27000          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49152          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49153          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49154          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49159          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49162          AB313SCS59:0           LISTENING
  TCP    0.0.0.0:49178          AB313SCS59:0           LISTENING
  TCP    127.0.0.1:5939         AB313SCS59:0           LISTENING
  TCP    127.0.0.1:8080         AB313SCS59:0           LISTENING
  TCP    127.0.0.1:8307         AB313SCS59:0           LISTENING
  TCP    127.0.0.1:27000        AB313SCS59:49173       ESTABLISHED
  TCP    127.0.0.1:49156        AB313SCS59:0           LISTENING
  TCP    127.0.0.1:49171        AB313SCS59:49172       ESTABLISHED
  TCP    127.0.0.1:49172        AB313SCS59:49171       ESTABLISHED
  TCP    127.0.0.1:49173        AB313SCS59:27000       ESTABLISHED
  TCP    172.16.8.94:139        AB313SCS59:0           LISTENING
  TCP    172.16.8.94:1521       AB313SCS59:49163       ESTABLISHED
  TCP    172.16.8.94:7279       AB313SCS59:49187       ESTABLISHED
  TCP    172.16.8.94:49163      AB313SCS59:1521        ESTABLISHED
  TCP    172.16.8.94:49187      AB313SCS59:7279        ESTABLISHED
  TCP    172.16.8.94:50948      maa05s02-in-f3:https   ESTABLISHED
  TCP    172.16.8.94:50949      maa05s02-in-f10:https  ESTABLISHED
  TCP    172.16.8.94:50951      maa05s01-in-f3:https   ESTABLISHED
  TCP    172.16.8.94:50952      maa05s01-in-f13:https  ESTABLISHED
  TCP    172.16.8.94:50953      74.125.24.99:https     ESTABLISHED
  TCP    172.16.8.94:50955      maa05s01-in-f3:https   ESTABLISHED
  TCP    172.16.8.94:50956      maa05s01-in-f14:https  ESTABLISHED
  TCP    172.16.8.94:50960      maa03s28-in-f3:https   ESTABLISHED
  TCP    172.16.8.94:50961      maa05s04-in-f3:https   ESTABLISHED
  TCP    172.16.8.94:50962      maa05s06-in-f2:https   ESTABLISHED
  TCP    172.16.8.94:50963      maa05s01-in-f3:https   ESTABLISHED
  TCP    192.168.56.1:139       AB313SCS59:0           LISTENING
  TCP    192.168.150.1:139      AB313SCS59:0           LISTENING
  TCP    192.168.162.1:139      AB313SCS59:0           LISTENING
  TCP    [::]:80                AB313SCS59:0           LISTENING
  TCP    [::]:135               AB313SCS59:0           LISTENING
  TCP    [::]:443               AB313SCS59:0           LISTENING
  TCP    [::]:445               AB313SCS59:0           LISTENING
  TCP    [::]:7279              AB313SCS59:0           LISTENING
  TCP    [::]:8082              AB313SCS59:0           LISTENING
  TCP    [::]:8083              AB313SCS59:0           LISTENING
  TCP    [::]:27000             AB313SCS59:0           LISTENING
  TCP    [::]:49152             AB313SCS59:0           LISTENING
  TCP    [::]:49153             AB313SCS59:0           LISTENING
  TCP    [::]:49154             AB313SCS59:0           LISTENING
  TCP    [::]:49159             AB313SCS59:0           LISTENING
```