GIAC Certified Forensic Analyst

Practical Assignment

Version 2.0
Option 1 : Analyze an image

Christian Chablais

1. Executive summary - Abstract

I have examined an image of a USB flashdrive which has been found in the cubicle of Mr Lawrence. I had to find if there were any data related to Ms Leila Conley concerns : she had been contacted on her private email by Mr Lawence, who became increasingly aggressive and eventually showed up in a coffee shop while she was with a friend.

After first look at the flashdrive I could list 3 documents - some texts which had been emailed to Ms Conley. After further examination I discovered that at least three files had been deleted, but could be recovered. Among them there was a map with the direction to the coffee shop where Mr. Lawrence showed up in the evening of October 28th. The second file recovered was a so called "sniffer" : it is a piece of software which allows to listen and capture all the traffic on a network. Its effect is similar to a phone tap.

My findings indicate that this software had been installed, probably directly on Ms. Conley computer, or very close to it, and that it has been used to capture the content of an email she sent using a private account at hotmail.com to a friend. The content of this email is the third recovered file, in which we can read that Ms Conley fixed an appointment in a coffee shop with a friend. The map has been downloaded shortly after.

You will find here after the steps of my examination with the detail of the files, both already present and recovered ; how I identified the sniffer and the way it was used to spy email the email sent by Ms Conley. The last two sections regard the legal implications and the recommendations for the system for the security administrator.

2. Examination details

2.1 Download and verification

The image file to be analyzed was downloaded from https://www.giac.org/GCFAPartical2.0-USBImageAndInfo.zip.gz. It was provided with the following chain of custody :

Tag #: USBDF-64531026-RL-001
Description : 64M Lexar Media Jumpdrive
Serial #: JDSP064-04-5000C
Image: USBFD-64531026-RL-001.img
MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5

The file was first saved on a XP workstation, then unzipped with the order :

```
   gunzip –N GCFAPractical2.0-USBImageAndInfo.zip.gz ;
```

note: the flag "-N" saves the original name and timestamp.

which generated the following output :

```
   26/10/2004  11:58        62'439'424 USBFD-64531026-RL-001.img
                  1 File(s)      62'439'424 bytes
```

The file " USBFD-64531026-RL-001.img" corresponds to name of the chain of custody.
I checked the md5sum of the file:

```
C:\giac\gcfa\practical>md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5 *USBFD-64531026-RL-001.img
```

It corresponds to the chain of custody output.

2.2 Transfer on the analyst station

It was the transferred on the analyst station, running the OS Linux Redhat 9, with the softwares "Sleuthkit 1.73" and "Autopsy 2.03" installed, in this way :

source XP: IP 192.168.109.1
destination Linux : IP 192.168.109.129, on the same C class subnet
on Linux I ran : `nc -l -p 3333 > USBFD-64531026-RL-001.img`
on XP : `dd if= USBFD-64531026-RL-001.img | nc  192.168.109.129 3333`

I then ran md5sum on the Linux station and got the same output as in the XP environment. The file had not been altered during the transfer.

2.3 Nature of the file

I got an idea of the nature of the file with:

command: `file USBFD-64531026-RL-001.img`
output : `x86 boot sector`

It is a physical image which contains one or more partitions.

2.4 Extract and mount the partitions contained in the file

Then I had to extract the logical partitions with :

```
mmls -t dos USBFD-64531026-RL-001.img
DOS Partition Table
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000031   0000000031   Unallocated
02:  00:00   0000000032   0000121950   0000121919   DOS FAT16 (0x04)
```

Three partitions are present. The interesting is the third one which was extracted on a file called "part1.dd" with :

```
dd if=USBFD-64531026-RL-001.img bs=512 skip=32 count=121919 of=part1.dd
121919+0 records in
121919+0 records out
62422528 bytes transferred in 0.694513 seconds (89879561 bytes/sec)
```

I could mount the partition with :

```
mount -o ro,loop part1.dd /mnt/gcfa/
```

note the flag "ro" is used to mount them in read only mode, so that data are not altered during the analysis. Result :

```
mount -l
/mnt/sda/images/gcfa/part1.dd on /mnt/gcfa type vfat (ro,loop=/dev/loop2)
```

It is interesting to note that the file system is FAT, which offers no security, but is widely recognized by heterogeneous systems, and therefore is a good choice for USB drives.

I took the mk5sum of the partition with :

```
md5sum part1.dd
5f830a763e2144483f78113a8844ad52  part1.dd
```

2.5 First look at the content

At first look there are three files on this image :

```
[root (gcfa)]# ls -al
drwxr--r--   2 root root 16384 Dec 31  1969 .
drwxr-xr-x  10 root root  1024 Jan 22 09:08 ..
-rwxr--r--   1 root root 19968 Oct 28 20:24 coffee.doc
-rwxr--r--   1 root root 19968 Oct 25 09:32 her.doc
-rwxr--r--   1 root root 19968 Oct 26 09:48 hey.doc

[root (gcfa)]# ls -lit
19 -rwxr--r--  1 root root 19968 Oct 28 20:24 coffee.doc
18 -rwxr--r--  1 root root 19968 Oct 26 09:48 hey.doc
17 -rwxr--r--  1 root root 19968 Oct 25 09:32 her.doc
```

The inode numbers are consecutive. It looks that the 3 files were created in order. At this point I do not know if other files had been present on the USB drive and deleted.

2.6 File system information

Those data are useful before proceeding further.

```
fsstat -f fat part1.dd
```

Output:

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT

OEM Name: MSWIN4.1
Volume ID: 0x0
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 32

File System Layout (in sectors)
Total Range: 0 - 121918
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 239
* FAT 1: 240 - 478
* Data Area: 479 - 121918
** Root Directory: 479 - 510
** Cluster Area: 511 - 121918

METADATA INFORMATION
--------------------------------------------
Range: 2 - 1942530
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 1024
```

```
Total Cluster Range: 2 - 60705

FAT CONTENTS (in sectors)
----------------------------------------------
511-550 (40) -> EOF
551-590 (40) -> EOF
591-630 (40) -> EOF
```

2.7 Load data in "Autopsy"

I added a new case, with the image part1.dd. In the file "analysis" section, I found the 3 ".doc" files and 7 deleted files. Basically "Autopsy" in a graphic interface to the Sleuthkit. So, at this point I preferred to go back to the command line and work with the Sleuthkit directly.

The goal was to find what files were or had been on this device and how they were related to the case of Mr. Lawrence.

2.8 What is present at the file system level ?

I got the list of those files, both regular and deleted, with :

```
fls -apr -f fat part1.dd
```

Output:

```
r/r 3:  her.doc
r/r 4:  hey.doc
r/r * 7:        WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 10:       WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 12:       WinDump.exe (_INDUMP.EXE)
r/r * 14:       WinDump.exe (_INDUMP.EXE)
r/r * 15:       _apture
r/r * 16:       _ap.gif
r/r * 17:       _ap.gif
r/r 18: coffee.doc
```

meaning of the flags : r=recursive; -a: Display "." and ".." entries; -p: Display full path for each file all files on the root.

There are no subdirectories :

```
fls -aD -f fat part1.dd
empty ; no subdir
```

From the above outputs I observe that the following inodes are missing : 1,2,5,6,8,9. What's more it would be interesting to see if any node above 18 contains data. This can be found by analyzing data at a lower level. It is also immediately clear at this point that the deleted data that were found with fls ("winpcap", "windump", "_apture","_ap.gif") must be recovered, if possible, and scrutinized. I chose to continue investigating for other data with at lower levels.

2.9 Inodes examination

2.9.1 Inodes (1) (2) and (19)

No usable information for (1)

```
istat -f fat part1.dd  1
Inode value is too small for image (2)
```

The inode (2) is the directory:

```
istat -f fat part1.dd  2
Directory Entry: 2
Allocated
File Attributes: Directory
Size: 16384
Name:

Directory Entry Times:
Written:        Thu Jan  1 01:00:00 1970
Accessed:       Thu Jan  1 01:00:00 1970
Created:        Thu Jan  1 01:00:00 1970

Sectors:
479 480 481 482 483 484 485 486
487 488 489 490 491 492 493 494
495 496 497 498 499 500 501 502
503 504 505 506 507 508 509 510
root Directory
```

The (19) in not an inode : the last file created is "coffee.doc" on inode 19.

```
istat -f fat part1.dd  19
/KNOPPIX/usr/local/sleuthkit-1.73/bin/istat: 19 is not an inode
not and inode ; the last file created is coffee.doc on inode 18
```

2.9.2 Other inodes

The same kind of examination was done about each inode with:

```
for i in 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 ; do istat -f fat part1 $i; done >
output/istat
```

The output generated is rather long and not published here. Here is a recapitulation:

A total of 16 files are found on the inodes 3 -> 18
3 inodes are allocated : (3)her.doc ; (4)hey.doc and (18) coffee.doc
13 inodes are not allocated
File recovery is not possible for 10 inodes : 5,6,7,8,9,10,11,12,13,16
File recover is possible for (14) (15) and (17)

2.10 Inodes recovery

The following 3 files were recovered, and the nature of their content was determined with the unix command "file".

2.10.1 windump.exe

```
icat -f fat -r part1.dd 14 | md5sum
79375b77975aa53a1b0507496107bff7  -

icat -f fat -r part1.dd 14 > output/windump.exe

 file windump.exe
windump.exe: MS-DOS executable (EXE), OS/2 or MS Windows
```

2.10.2 capture

```
icat -f fat -r part1.dd 15 | md5sum
2097b7b0a9fedb4238b67e976c4ae1cb  -

icat -f fat -r part1.dd 15 > output/capture
```

```
file capture
capture: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)
```

2.10.3 capture

```
icat -f fat -r part1.dd 17 | md5sum
9bc3923cf8e72fd405d7cea8c8781011  -

icat -f fat -r part1.dd 17 > output/_ap.gif

file _ap.gif
_ap.gif: GIF image data, version 89a, 300 x 200
```

File recover was NOT possible for WinPcap_3_1_beta_3.exe.

2.11 Other disk space

Whatever has not been recovered so far is, from my point of view, a bulk of unstructured data. But it is interested to save it for later analysis. Typically I will run a "dirty words" list search, based on what I may have learned, and something might or might not show up.

2.11.1 slackspace

```
dls –f fat –s part1.dd > output/part1.slack
```

the flag –s instructs to look for slack space only

2.11.2 unallocated space

```
dls –f fat part1.dd > output/part1.dls
```

2.12 Summary of extracted data

A md5sum was calculated on all the extracted data with :

```
find . -type f -exec md5sum "{}" ";"
```

The result in displayed in "section 3 Image details"

2.13 Timeline creation

The timeline was created using autopsy. Commands used from the autopsy log :

```
Thu Feb 10 12:16:55 2005: '/usr/local/sleuthkit-1.73/bin/fls'  -s 0 -m 'E:\' -f fat -r
'/mnt/sda/evidence/gcfa/usbfd/images/part1.dd' >>
'/mnt/sda/evidence/gcfa/usbfd/output/body'

Thu Feb 10 12:16:55 2005: '/usr/local/sleuthkit-1.73/bin/ils' -s 0 -m -f fat
'/mnt/sda/evidence/gcfa/usbfd/images/part1.dd' >>
'/mnt/sda/evidence/gcfa/usbfd/output/body'

Thu Feb 10 12:18:25 2005: LANG=C LC_ALL=C '/usr/local/sleuthkit-1.73/bin/mactime' -b
'/mnt/sda/evidence/gcfa/usbfd/output/body'  -i day
'/mnt/sda/evidence/gcfa/usbfd/output/timeline.txt.sum'   >
'/mnt/sda/evidence/gcfa/usbfd/output/timeline.txt'

Thu Feb 10 12:18:25 2005: '/usr/local/sleuthkit-1.73/bin/md5'
'/mnt/sda/evidence/gcfa/usbfd/output/timeline.txt'
```

2.14 Overview of the file contents

I started looking at the content of the files. Details about the files are listed in the next section. Here is a summary of each of them as they appear in the timeline.

2.13.1 "her.doc" : it is a Microsoft Office Document created on Mon Oct 25. I opened it with MS Word 97. It is a simple text written by Mr. Lawrence who invited somebody for dinner – a flirt message.

2.13.2 "hey.doc" : it is a Microsoft Office Document created the day after. It is a second invitation, for a coffee this time.

2.13.3 "windump.exe" : it is a MS-DOS executable (EXE), OS/2 or MS Windows which has been recovered. It appears first in the time line on Wed 27 oct. I ran " `strings windump.exe | wc -l` ", computed its md5sum. It was rather easy to discover the nature of the software (details are listed in section "4. Program identification"). Windump is the port of "tcpdump", a Unix sniffer, to Windows (1).

2.13.4 "capture" : was created on Thu Oct 28. The "`file`" command indicates it is a "capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)". This file has been created by windump installed previously and its content is the data sniffed on the wire. This is the most interesting part of the forensic analysis, which is detailed in section "5. Forensic details". In summary it appears here that Mr. Lawrence has captured a private email sent by Mrs Leila, who invites a friend of her at the coffee shop on the corner Hollywood and McCadden. She used an hotmail account.

2.13.5 "_ap.gif" : it is a GIF image data. Basically it is a map which indicates the location of the coffee shop on the corner Hollywood and McCadden. It has been created after the "capture" file, and then deleted. From this timeline I can deduce that Mr. Lawrence has read the content of the email, that he understood that an appointment has been fixed and he wanted to know where exactly, so he downloaded a map of the place.

2.13.5 "coffee.doc" : a Microsoft Office Document created on Thu Oct 28 at 19:24. Mr. Lawrence is bitter because he saw "here" with somebody else.

My findings fit with Ms Conlay concerns : Leila Conlay complained that Robert appeared at a coffe shop where she was with a friend on Octobre 28th and that his emails became more aggressive.

In the "Forensic details" I try know more about what, where and when things happened. This is the basic to determine the legal implications, my corrective recommendations and a guideline do dig into the slack spade and unallocated data bulk.

2.15 Unallocated space

2.15.1 dirty words list
I found those interested words in the "capture" file and added them in the dirty words list : "
`Hollywood Frankline Ave Hollywood Blvd Hawthorn Sunset Longpre Selma Highland Wilcox Vine`

`Argile coffee Leila Conlay`". The command " `strings part1.dls | grep -i -f dirtywords` " gave a large output, which is similar to what I get with " `strings part1.dls | grep -i -f dirtywords` ". This means that content of the file "capture" is also present in the allocated space. It is a good new : as I already can analyze the " capture " file, I will not miss data.
The same command run on the slack space gave no result. Even " strings " gave nothing interesting.

2.15.2 looking for "winpcap"
The " WinPcap_3_1_beta_3.exe " had been present of the file system but it was not possible to recover it. "Winpcap" is the companion of "Windump", and it must be installed before windump can be run. I wanted to find a trace of this software to make sure that "windump" had been run from this file file system.

It appeared from " Istat " that the range of blocks 591 – 1540 were unalocated. I extracted them with " `dcat -f fat part1.dd 591 949 > output/orphanblocks` ". I found 6142 results with the command " `strings orphanblocks | wc -l` ". To minimize the field, I downloaded the file " WinPcap_3_1_beta4.exe " from the windump site [***]. It is not exactly " WinPcap_3_1_beta_3.exe " – I could not locate it – but close enough. I ran " strings " on this file and compared both output. I found similarities between both, like :
"

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><assembly manifestVersion="1.0"
xmlns="urn:schemas-m
icrosoft-com:asm.v1"><assemblyIdentity processorArchitecture="*" version="5.1.0.0"
type="win32" name="Micro
soft.Windows.Shell.shell32"/><description>Windows
Shell</description><dependency><dependentAssembly><assemb
lyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0"
publicKeyToken="6595b641
44ccf1df" language="*" processorArchitecture="*"/></dependentAssembly></dependency></assembly>
KERNEL32.DLL
advapi32.dll
comctl32.dll
gdi32.dll
ole32.dll
oleaut32.dll
shell32.dll
user32.dll
version.dll
LoadLibraryA
GetProcAddress
ExitProcess
RegCloseKey
```

"
It was close enough to suppose that "winpcap" had been present on the USB drive, but not 100% sure. What is sure it that "windump" has been run and that without "winpcap" it would not have been able to produce the "capture" file. So this is not so relevant for this case.

2.15.3 Other data ?
I tried to find something with the software "fatback" but got nothing more. I tried then to isolate every single block and run " file " on it with the following python script called " blocksid "

```
#!//usr/bin/python
import os
```

```
# 591-1541
# for i in range(591,1541):
for i in range(591,1542):
    os.system("echo %(i)s: | tr -d '\n'" % vars())
    os.system("dcat -f fat /mnt/sda/images/gcfa/part1.dd %(i)s 1| file -" % vars())
```

which is run with :

```
./blocksid >> /mnt/sda/images/gcfa/output/file-to-orphan-blocks
```

I only found a copy of "coffee.doc" and some garbage. At this point I assume I had all the data.

3. Image details

3.1 List of the files in the image with their md5sum

```
9785a777c5286738f9deb73d8bc57978  ./her.doc
ca601d4f8138717dca4de07a8ec19ed1  ./hey.doc
79375b77975aa53a1b0507496107bff7  ./windump.exe (recovered)
2097b7b0a9fedb4238b67e976c4ae1cb  ./capture (recovered)
9bc3923cf8e72fd405d7cea8c8781011  ./_ap.gif (recovered)
a833c58689596eda15a27c931e0c76d1  ./coffee.doc
```

The 3 files "windump.exe", "capture" and "_ap.gif" had been deleted by Mr. Lawrence and have been recovered.

3.2 Files details

3.2.1 her.doc

```
Directory Entry: 3
Allocated
File Attributes: File, Archive
Size: 19968
Name: her.doc

Directory Entry Times:
Written:   Mon Oct 25 08:32:08 2004
Accessed:  Mon Oct 25 00:00:00 2004
Created:   Mon Oct 25 08:32:06 2004

Sectors:
511 512 513 514 515 516 517 518
519 520 521 522 523 524 525 526
527 528 529 530 531 532 533 534
535 536 537 538 539 540 541 542
543 544 545 546 547 548 549 550

file her.doc
her.doc: Microsoft Office Document
```

Content :

"

```
Hey I saw you the other day.  I tried to say "hi", but you disappeared???  That
was a nice blue dress you were wearing.  I heard that your car was giving you
some trouble.  Maybe I can give you a ride to work sometime, or maybe we can
get dinner sometime?

Have a nice day
```

"

3.2.2 hey.doc

```
   Directory Entry: 4
   Allocated
   File Attributes: File, Archive
   Size: 19968
   Name: hey.doc

   Directory Entry Times:
   Written:   Tue Oct 26 08:48:10 2004
   Accessed:  Tue Oct 26 00:00:00 2004
   Created:   Tue Oct 26 08:48:06 2004

   Sectors:
   551 552 553 554 555 556 557 558
   559 560 561 562 563 564 565 566
   567 568 569 570 571 572 573 574
   575 576 577 578 579 580 581 582
   583 584 585 586 587 588 589 590

   file hey.doc
   hey.doc: Microsoft Office Document
```

Content :

```
"
Hey!  Why are you being so mean?  I was just offering to help you out with your
car!  Don't tell me to get lost!  You should give me a chance.  I'm a nice guy
just trying to help you out, just because I think you're cute doesn't mean I'm
weird.  Perhaps coffee would be better, when would be a good time for you?
"
```

3.2.3 windump.exe

```
   Directory Entry: 14
   Not Allocated
   File Attributes: File, Archive
   Size: 450560
   Name: _INDUMP.EXE

   Directory Entry Times:
   Written:   Wed Oct 27 16:24:02 2004
   Accessed:  Thu Oct 28 00:00:00 2004
   Created:   Wed Oct 27 16:24:04 2004

   Sectors:
   1541 1542

   Recovery:
   1541 1542 1543 1544 1545 1546 1547 1548
   1549 1550 1551 1552 1553 1554 1555 1556
   1557 1558 1559 1560 1561 1562 1563 1564
   1565 1566 1567 1568 1569 1570 1571 1572
   1573 1574 1575 1576 1577 1578 1579 1580
   1581 1582 1583 1584 1585 1586 1587 1588
   1589 1590 1591 1592 1593 1594 1595 1596
   1597 1598 1599 1600 1601 1602 1603 1604
   1605 1606 1607 1608 1609 1610 1611 1612
   1613 1614 1615 1616 1617 1618 1619 1620
   1621 1622 1623 1624 1625 1626 1627 1628
   1629 1630 1631 1632 1633 1634 1635 1636
   1637 1638 1639 1640 1641 1642 1643 1644
   1645 1646 1647 1648 1649 1650 1651 1652
```

```
1653 1654 1655 1656 1657 1658 1659 1660
1661 1662 1663 1664 1665 1666 1667 1668
1669 1670 1671 1672 1673 1674 1675 1676
1677 1678 1679 1680 1681 1682 1683 1684
1685 1686 1687 1688 1689 1690 1691 1692
1693 1694 1695 1696 1697 1698 1699 1700
1701 1702 1703 1704 1705 1706 1707 1708
1709 1710 1711 1712 1713 1714 1715 1716
1717 1718 1719 1720 1721 1722 1723 1724
1725 1726 1727 1728 1729 1730 1731 1732
1733 1734 1735 1736 1737 1738 1739 1740
1741 1742 1743 1744 1745 1746 1747 1748
1749 1750 1751 1752 1753 1754 1755 1756
1757 1758 1759 1760 1761 1762 1763 1764
1765 1766 1767 1768 1769 1770 1771 1772
1773 1774 1775 1776 1777 1778 1779 1780
1781 1782 1783 1784 1785 1786 1787 1788
1789 1790 1791 1792 1793 1794 1795 1796
1797 1798 1799 1800 1801 1802 1803 1804
1805 1806 1807 1808 1809 1810 1811 1812
1813 1814 1815 1816 1817 1818 1819 1820
1821 1822 1823 1824 1825 1826 1827 1828
1829 1830 1831 1832 1833 1834 1835 1836
1837 1838 1839 1840 1841 1842 1843 1844
1845 1846 1847 1848 1849 1850 1851 1852
1853 1854 1855 1856 1857 1858 1859 1860
1861 1862 1863 1864 1865 1866 1867 1868
1869 1870 1871 1872 1873 1874 1875 1876
1877 1878 1879 1880 1881 1882 1883 1884
1885 1886 1887 1888 1889 1890 1891 1892
1893 1894 1895 1896 1897 1898 1899 1900
1901 1902 1903 1904 1905 1906 1907 1908
1909 1910 1911 1912 1913 1914 1915 1916
1917 1918 1919 1920 1921 1922 1923 1924
1925 1926 1927 1928 1929 1930 1931 1932
1933 1934 1935 1936 1937 1938 1939 1940
1941 1942 1943 1944 1945 1946 1947 1948
1949 1950 1951 1952 1953 1954 1955 1956
1957 1958 1959 1960 1961 1962 1963 1964
1965 1966 1967 1968 1969 1970 1971 1972
1973 1974 1975 1976 1977 1978 1979 1980
1981 1982 1983 1984 1985 1986 1987 1988
1989 1990 1991 1992 1993 1994 1995 1996
1997 1998 1999 2000 2001 2002 2003 2004
2005 2006 2007 2008 2009 2010 2011 2012
2013 2014 2015 2016 2017 2018 2019 2020
2021 2022 2023 2024 2025 2026 2027 2028
2029 2030 2031 2032 2033 2034 2035 2036
2037 2038 2039 2040 2041 2042 2043 2044
2045 2046 2047 2048 2049 2050 2051 2052
2053 2054 2055 2056 2057 2058 2059 2060
2061 2062 2063 2064 2065 2066 2067 2068
2069 2070 2071 2072 2073 2074 2075 2076
2077 2078 2079 2080 2081 2082 2083 2084
2085 2086 2087 2088 2089 2090 2091 2092
2093 2094 2095 2096 2097 2098 2099 2100
2101 2102 2103 2104 2105 2106 2107 2108
2109 2110 2111 2112 2113 2114 2115 2116
2117 2118 2119 2120 2121 2122 2123 2124
2125 2126 2127 2128 2129 2130 2131 2132
2133 2134 2135 2136 2137 2138 2139 2140
2141 2142 2143 2144 2145 2146 2147 2148
2149 2150 2151 2152 2153 2154 2155 2156
2157 2158 2159 2160 2161 2162 2163 2164
2165 2166 2167 2168 2169 2170 2171 2172
```

```
2173 2174 2175 2176 2177 2178 2179 2180
2181 2182 2183 2184 2185 2186 2187 2188
2189 2190 2191 2192 2193 2194 2195 2196
2197 2198 2199 2200 2201 2202 2203 2204
2205 2206 2207 2208 2209 2210 2211 2212
2213 2214 2215 2216 2217 2218 2219 2220
2221 2222 2223 2224 2225 2226 2227 2228
2229 2230 2231 2232 2233 2234 2235 2236
2237 2238 2239 2240 2241 2242 2243 2244
2245 2246 2247 2248 2249 2250 2251 2252
2253 2254 2255 2256 2257 2258 2259 2260
2261 2262 2263 2264 2265 2266 2267 2268
2269 2270 2271 2272 2273 2274 2275 2276
2277 2278 2279 2280 2281 2282 2283 2284
2285 2286 2287 2288 2289 2290 2291 2292
2293 2294 2295 2296 2297 2298 2299 2300
2301 2302 2303 2304 2305 2306 2307 2308
2309 2310 2311 2312 2313 2314 2315 2316
2317 2318 2319 2320 2321 2322 2323 2324
2325 2326 2327 2328 2329 2330 2331 2332
2333 2334 2335 2336 2337 2338 2339 2340
2341 2342 2343 2344 2345 2346 2347 2348
2349 2350 2351 2352 2353 2354 2355 2356
2357 2358 2359 2360 2361 2362 2363 2364
2365 2366 2367 2368 2369 2370 2371 2372
2373 2374 2375 2376 2377 2378 2379 2380
2381 2382 2383 2384 2385 2386 2387 2388
2389 2390 2391 2392 2393 2394 2395 2396
2397 2398 2399 2400 2401 2402 2403 2404
2405 2406 2407 2408 2409 2410 2411 2412
2413 2414 2415 2416 2417 2418 2419 2420
file windump.exe
windump.exe: MS-DOS executable (EXE), OS/2 or MS Windows
```

Strings :

```
@(#) $Header: /tcpdump/master/tcpdump/addrtoname.c,v 1.96.2.6 2004/03/24 04:14:31 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/bpf_dump.c,v 1.14.2.2 2003/11/16 08:51:04 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/datalinks.c,v 1.1.2.3 2003/11/16 09:29:48 guy Exp $
(LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/dlnames.c,v 1.2.2.3 2003/11/18 23:12:12 guy Exp $
(LBL)
@(#) $Header: /tcpdump/master/tcpdump/gmpls.c,v 1.2.2.2 2003/11/16 08:51:05 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/gmt2local.c,v 1.7.2.2 2003/11/16 08:51:06 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_aton.c,v 1.4.2.2 2003/11/16 08:52:01 guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_ntop.c,v 1.5.2.2 2003/11/16 08:52:01 guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_pton.c,v 1.4.2.2 2003/11/16 08:52:01 guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/machdep.c,v 1.10.2.3 2003/12/15 03:53:42 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/oui.c,v 1.2.2.1 2004/02/06 14:38:51 hannes Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/parsenfsfh.c,v 1.25.2.2 2003/11/16 08:51:07 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-802_11.c,v 1.22.2.6 2003/12/10 09:52:33 guy Exp $ (LBL)
?@(#) $Header: /tcpdump/master/tcpdump/print-ah.c,v 1.19.2.3 2003/11/19 00:35:43 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-aodv.c,v 1.8.2.3 2004/03/24 00:30:41 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-ap1394.c,v 1.1.2.1 2004/03/17 22:15:53 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-arcnet.c,v 1.15.2.2 2003/11/16 08:51:09 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-arp.c,v 1.61.2.2 2003/11/16 08:51:10 guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/print-ascii.c,v 1.10.2.3 2003/12/29 22:42:20 hannes Exp $
@(#) $Header: /tcpdump/master/tcpdump/print-atalk.c,v 1.78.2.2 2003/11/16 08:51:11 guy Exp $ (LBL)
[... etc ... (similar pattern)]
H:mm:ss
dddd, MMMM dd, yyyy
M/d/yy
December
November
October
[... etc ...]
Microsoft Visual C++ Runtime Library
FreeLibrary
```

```
GetProcAddress
LoadLibraryA
GetSystemDirectoryA
KERNEL32.dll
WSOCK32.dll
endservent
getservent
eproto_db
pcap_next_etherent
bpf_image
pcap_datalink
pcap_loop
pcap_dump_open
pcap_setfilter
pcap_close
pcap_compile
pcap_lookupnet
pcap_snapshot
pcap_geterr
pcap_setbuff
pcap_open_live
pcap_lookupdev
pcap_open_offline
pcap_findalldevs
wsockinit
pcap_file
pcap_stats
pcap_dump_flush
pcap_dump
pcap_dump_close
[...etc...]
```

3.2.4 capture

```
Directory Entry: 15
Not Allocated
File Attributes: File, Archive
Size: 53056
Name: _apture

Directory Entry Times:
Written:   Thu Oct 28 11:11:00 2004
Accessed:  Thu Oct 28 00:00:00 2004
Created:   Thu Oct 28 11:08:24 2004

Sectors:
2421 2422

Recovery:
2421 2422 2423 2424 2425 2426 2427 2428
2429 2430 2431 2432 2433 2434 2435 2436
2437 2438 2439 2440 2441 2442 2443 2444
2445 2446 2447 2448 2449 2450 2451 2452
2453 2454 2455 2456 2457 2458 2459 2460
2461 2462 2463 2464 2465 2466 2467 2468
2469 2470 2471 2472 2473 2474 2475 2476
2477 2478 2479 2480 2481 2482 2483 2484
2485 2486 2487 2488 2489 2490 2491 2492
2493 2494 2495 2496 2497 2498 2499 2500
2501 2502 2503 2504 2505 2506 2507 2508
2509 2510 2511 2512 2513 2514 2515 2516
2517 2518 2519 2520 2521 2522 2523 2524

file capture
capture: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)
```

Strings :

```
AP),
AP),
x+,0
public
'@out 192.168.2.104 2038 64.4.34.250 80
AP),
AP),
AP),
POST /cgi-bin/premail/2452 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint, applicatio
n/msword, */*
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-
bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029263cd9
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com
Content-Length: 576
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1;
MSPAuth=5Qr3f0LU3B54zQBmCG3iUtdaiAo608EFiBYmrtzv6oAL1cQ1ayApRce4N7XC
Ekk%2aa5e9H9cWS5x%21xBTivKy%2aSEwg%24%24;
MSPProf=5e1XcTCShGOf1gQhcClTXJM67JMAbywIG67BmEwf%2aNbKWq2vOyMjJTO2P1%2aaU%2aviMTcr8nes
tOX6uJi5QYv9nb%21V3ReGZPm3yhrewvAYzs3vjyK4rdsGyuC2UGGRIga01ksxgsOTye%2aN6x6RSiEoVSY1B7nwcTw
qlcErZoYBZYceDYvmlHy2W1RBkki3tMoJtq2I
N4ZFwblNM%24;
PIM=1%2clang%2cEN%2ctabstyle%2c4%2ccluster%2cby12fd%252ebay12%252ehotmail%252emsn%252ecom%2
ctimestamp%2c1098692237
%2csection%2cpersonal%2csubsection%2cInvalidSubSection; mid=29ede1b79f320aa332327a4460;
HMSatchmo=0; HMP1=1; HMSC0899=224flowerg
irl96%40hotmail%2ecomrEM%2a5jEHcXVGV4%2aAWzQ6w%2a0KAj39KgAbJwM3dx89O12eFCP8QpvDRxtOmG0LfDW%
2azTT3QAp7%2aslY6H2QtQ5HQXNkLZglQmXIy
9iEXRtDjJoz9OYjoxLF3Ma%2axDVQGszV4go%2au43pw8jYIglxM0UW%21z0ldqqhUN1TQ4ctSsc5TvwyIbDyDgcRpT
SWI4a5eks5.6
AP),
[... etc ...]
```

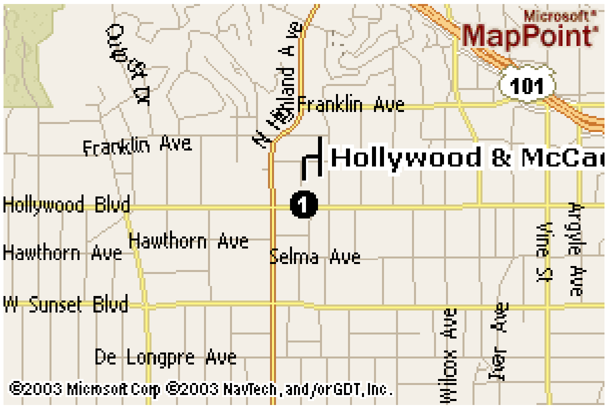
More details about the content of this file in the "Forensic details" section

3.2.5 _ap.gif : used a "map.gif" by Mr. Lawrence

```
Directory Entry: 17
Not Allocated
File Attributes: File, Archive
Size: 8814
Name: _ap.gif

Directory Entry Times:
Written:	Thu Oct 28 11:17:46 2004
Accessed:	Thu Oct 28 00:00:00 2004
Created:	Thu Oct 28 11:17:44 2004

Sectors:
2525 2526

Recovery:
2525 2526 2527 2528 2529 2530 2531 2532
2533 2534 2535 2536 2537 2538 2539 2540
```

```
2541 2542

file _ap.gif
_ap.gif: GIF image data, version 89a, 300 x 200
```

Content :



3.2.5 coffee.doc

```
Directory Entry: 18
Allocated
File Attributes: File, Archive
Size: 19968
Name: coffee.doc

Directory Entry Times:
Written:   Thu Oct 28 19:24:48 2004
Accessed:  Thu Oct 28 00:00:00 2004
Created:   Thu Oct 28 19:24:46 2004

Sectors:
591 592 593 594 595 596 597 598
599 600 601 602 603 604 605 606
607 608 609 610 611 612 613 614
615 616 617 618 619 620 621 622
623 624 625 626 627 628 629 630

/KNOPPIX/usr/local/sleuthkit-1.73/bin/icat -f fat -r part1.dd 18 | md5sum
a833c58689596eda15a27c931e0c76d1  -

file coffee.doc
coffee.doc: Microsoft Office Document
```

Content :

```
"
Hey what gives?  I was drinking a coffee on thursday and saw you stop buy with
some guy!  You said you didn't want coffee with me, but you'll go have it with
some random guy???  He looked like a loser!  Guys like that are nothing but
trouble.  I can't believe you did this to me!  You should stick to your word,
if you're not interested in going to coffee with me then you shouldn't be going
with anyone!  I heard rumors about a "bad batch" of coffee, hope you don't get
any...
"
```

3.3 Note about the File owner

The file owner of all these files is not listed here. It is always "root" ! The reason is that it is a FAT file system which has no security for user access, therefore no reason to display it.

4. Program identification

Mr. Lawrence use the program WINDUMP.EXE, which is widely known as the port of the Linux sniffer TCPDUMP. This software should be used by network administrators to observe the traffic on the wire. But it can be used too as a spy tool to gain whatever information going thgrough the network.

WINDUMP is an open source software which can be freely downloaded at http://windump.polito.it/ . I downloaded the current version as at Apri 15 which was "WinDump 3.8.3 beta " and ran md5sum on it :

```
   C:\xxx\windump>md5sum WinDump.exe
   79375b77975aa53a1b0507496107bff7 *WinDump.exe
```

The md5 checksum of this files corresponds to the "`79375b77975aa53a1b0507496107bff7`" computed from the recovered file. As http://windump.polito.it/ is a reliable website I assume that it is the same software.

What's more the source of this software can be freely downloaded from this website and has been widely scrutinized by the community. So I think it is not necessary to re-compile it and observe its behaviour. I will rather concentrate on when it was used by Mr. Lawrence and analyze the data have been captured.

5. Forensic details

WINDUMP.EXE appears in two inodes : 12 and 14 together with "WINPCAP" for the first time on Wed October 27, after the first two documents. Windump has the capability to sniff traffic on the wire and save it to a file when run with the "-w" flag. As the file "capture" has been created as at " `Thu Oct 28 11:08:24 2004`" I assume that Mr. Laurence ran a similar command : " `windump -n -w capture` " at this moment.
The files WINDUMP, CAPTURE, WINPCAP and MAP.GIF have been deleted by Mr Lawrence, probably in an attempt to hide traces. They all could be recovered and CAPTURE is full of informations.

The "strings" analysis has been truncated because it was too space consuming, but at first sight some web traffic can be noticed. Here are further steps to discover the content of this file (2) :

5.1 look for IP addresses with "sstrings"

```
   sstrings -a -t d capture | grep -i -E "[0-2]?[[:digit:]]{1,22]?[[:digit:]]{1,2}\.[0-
   2]?[[:digit:]]{1,2}\.[0-2]?[[:digit:]]{1,2} 7 wc -l
```

20 hits found, all hidden within html code

5.2 Wich sessions have been captured ?
5.2.1 which protocols have been captured in the file?
As it is a tcpdump file, it can be analyzed with its own tool.

How many records in the file?

```
[root (output)]# tcpdump -nr capture | wc -l
reading from file capture, link-type EN10MB (Ethernet)
113
```

tcp traffic:

```
[root (output)]# tcpdump -nr capture tcp | wc -l
reading from file capture, link-type EN10MB (Ethernet)
107
```

udp traffic:

```
[root (output)]# tcpdump -nr capture udp | wc -l
reading from file capture, link-type EN10MB (Ethernet)
6
```

5.2.2 what kind of UDP traffic ?

Which IP source :

```
[root (output)]# tcpdump -nr capture udp | awk '{print $3}'
reading from file capture, link-type EN10MB (Ethernet)
192.168.2.1.2769
192.168.2.1.2770
192.168.2.1.2771
192.168.2.1.2772
192.168.2.1.2773
192.168.2.1.2774
```

Therefore all the traffic comes from an unique source: `192.168.2.1`

To which destination ? "

```
[root (output)]# tcpdump -nr capture udp | awk '{print $5}'
reading from file capture, link-type EN10MB (Ethernet)
192.168.2.255.162:
192.168.2.255.162:
192.168.2.255.162:
192.168.2.255.162:
192.168.2.255.162:
192.168.2.255.162:
```

UDP traffic summary :

- all packets come from 192.168.2.1 + ephemeral port > 192.168.2.255 (this is a broadcast) port 162 (snmp trap).
- as 192.168.2.255 is the broadcast, the net is 192.168.2.0/24
- we are on a private net ; this is an internal traffic

5.2.3 which kind of TCP traffic ?

Which IP sources ?

```
[root (output)]# tcpdump -nr capture tcp | awk '{ print $3}' | sort | uniq
reading from file capture, link-type EN10MB (Ethernet)
192.168.2.104.2038
192.168.2.104.2039
192.168.2.104.2040
192.168.2.104.2041
192.168.2.104.2042
192.168.2.104.2043
192.168.2.104.2044
192.168.2.104.2045
```

```
192.168.2.104.2046
207.68.177.124.80
207.68.178.16.80
216.73.86.40.80
63.209.188.62.80
64.4.34.250.80
```

To which destinations ?

```
 [root (output)]# tcpdump -nr capture tcp | awk '{ print $5}' | sort | uniq
reading from file capture, link-type EN10MB (Ethernet)

192.168.2.104.2038:
192.168.2.104.2039:
192.168.2.104.2040:
192.168.2.104.2041:
192.168.2.104.2042:
192.168.2.104.2043:
192.168.2.104.2044:
192.168.2.104.2045:
207.68.177.124.80:
207.68.178.16.80:
216.73.86.40.80:
63.166.13.75.80:
63.209.188.62.80:
64.4.34.250.80:
```

any traffic that does not involve 192.168.2.104 ?

```
[root (output)]# tcpdump -nr capture tcp and host 192.168.2.104 | wc -l
reading from file capture, link-type EN10MB (Ethernet)
107"
```

No, 192.168.2.104 is involved on every record

any traffic not on port 80 (http) ?

```
[root (output)]# tcpdump -nr capture tcp and host 192.168.2.104 and port 80 | wc -l
reading from file capture, link-type EN10MB (Ethernet)
107
```

No, this is all http traffic

The http hosts are:

```
207.68.177.124
207.68.178.16
216.73.86.40
63.166.13.75
63.209.188.62
64.4.34.250
```

5.3 Which kind of hosts are involved ?

I used p0f (3):

```
C:\tools\p0f\binary>p0f -s \giac\gcfa\practical\lab\capture
p0f - passive os fingerprinting utility, version 2.0.4-beta1
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
WIN32 port (C) M. Davis <mike@datanerds.net>, K. Kuehl <kkuehl@cisco.c
p0f: listening (SYN) on '\giac\gcfa\practical\lab\capture', 207 sigs (
), rule: 'all'.
192.168.2.104:2038 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 64.4.34.250:80 (distance 0, link: ethernet/modem)
192.168.2.104:2039 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 207.68.178.16:80 (distance 0, link: ethernet/modem)
192.168.2.104:2040 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
```

```
  -> 207.68.178.16:80 (distance 0, link: ethernet/modem)
192.168.2.104:2041 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 207.68.177.124:80 (distance 0, link: ethernet/modem)
192.168.2.104:2042 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 63.209.188.62:80 (distance 0, link: ethernet/modem)
192.168.2.104:2043 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 63.209.188.62:80 (distance 0, link: ethernet/modem)
192.168.2.104:2044 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 216.73.86.40:80 (distance 0, link: ethernet/modem)
192.168.2.104:2045 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 216.73.86.40:80 (distance 0, link: ethernet/modem)
192.168.2.104:2046 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
  -> 63.166.13.75:80 (distance 0, link: ethernet/modem)
[+] End of input file.
```

This is a Windows 2000 SP2+ or XP SP1 machine ; only broadcasts and traffic related to the host 192.168.2.104 traffic was captured

5.4 Where was the sniffer placed ?

TTL (Time To Live) analysis

```
[root (output)]# tcpdump -nvr capture src host 192.168.2.104 | more
reading from file capture, link-type EN10MB (Ethernet)
19:10:54.088558 IP (tos 0x0, ttl 128, id 38853, offset 0, flags [DF], length: 48) 192.
168.2.104.2038 > 64.4.34.250.80: S [tcp sum ok] 4044750885:4044750885(0) win 16384 <ms
s 1460,nop,nop,sackOK>
19:10:54.112831 IP (tos 0x0, ttl 128, id 38855, offset 0, flags [DF], length: 40) 192.
168.2.104.2038 > 64.4.34.250.80: . [tcp sum ok] ack 3465097624 win 17520
19:10:54.113010 IP (tos 0x0, ttl 128, id 38856, offset 0, flags [DF], length: 1500) 19
2.168.2.104.2038 > 64.4.34.250.80: . [tcp sum ok] 0:1460(1460) ack 1 win 17520
19:10:54.113030 IP (tos 0x0, ttl 128, id 38857, offset 0, flags [DF], length: 316) 192
.168.2.104.2038 > 64.4.34.250.80: P [tcp sum ok] 1460:1736(276) ack 1 win 17520
19:10:54.113055 IP (tos 0x0, ttl 128, id 38858, offset 0, flags [DF], length: 616) 192
.168.2.104.2038 > 64.4.34.250.80: P [tcp sum ok] 1736:2312(576) ack 1 win 17520
19:10:54.224430 IP (tos 0x0, ttl 128, id 38861, offset 0, flags [DF], length: 40) 192.
168.2.104.2038 > 64.4.34.250.80: . [tcp sum ok] ack 361 win 17160
```

considerations

a) The TTL value of the packets originated by 192.168.2.104 is always 128. The TTL field initial value is decremented at every gateway the packet crosses. 128 is a typical starting value for ttl (this varies from OS to OS). So the sniffer is placed on the same physical subnet as 192.168.2.104.

b) possibility exists that the captured traffic has been filtered, because we do not see traffic with other hosts on the net. In fact only traffic with 192.168.2.104 is present.

two possibilities

b) the first option is that the host with the sniffer was installed on a **hub** where the target (192.168.2.104) was connected to. It is the nature of hubs to repeat traffic on every port. The sysadmin can answer this. This is unlikely because hubs are not that usual nowadays, they are rather replaced by switches which do not send traffic to every port.

c) but most probably the sniffer has been installed directly on the Leila Conley's computer. Mr Lawrence could have plugged the usb key on the target machine, run windump with flag "windump.exe -w capture", which writes the sniffed traffic on the "capture" file for later analysis. He probably came after she left to take the USB key and read its content.

It is also possible that he copied the files from the USB to the computer, then ran them, and then copied them back to the USB drive. The computer of Ms. Conley should be examined to answer definitively. What is sure is that the sniffer was VERY CLOSE to the victim.

Anyway I know now that interesting data were on the HTTP traffic of the CAPTURE file.

5.5 HTTP sessions

5.5.1 which sessions are present ?

```
[root (output)]# tcpdump -nr capture tcp and src host 192.168.2.104 | awk '{print $3}' |
awk -F "." '{print| sort | uniq
reading from file capture, link-type EN10MB (Ethernet)
2038
2039
2040
2041
2042
2043
2044
2045
2046
```

which sessions were originated (with syn) ?

```
[root (output)]# tcpdump -nr capture tcp[13]=0x2
reading from file capture, link-type EN10MB (Ethernet)
19:10:54.088558 IP 192.168.2.104.2038 > 64.4.34.250.80: S 4044750885:4044750885(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.369232 IP 192.168.2.104.2039 > 207.68.178.16.80: S 4044886046:4044886046(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.372242 IP 192.168.2.104.2040 > 207.68.178.16.80: S 4044949957:4044949957(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.446785 IP 192.168.2.104.2041 > 207.68.177.124.80: S 4044982971:4044982971(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.492078 IP 192.168.2.104.2042 > 63.209.188.62.80: S 4045056566:4045056566(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.566497 IP 192.168.2.104.2043 > 63.209.188.62.80: S 4045141580:4045141580(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.642292 IP 192.168.2.104.2044 > 216.73.86.40.80: S 4045197376:4045197376(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.652734 IP 192.168.2.104.2045 > 216.73.86.40.80: S 4045239291:4045239291(0) win
16384 <mss 1460,nop,nop,sackOK>
19:10:54.960378 IP 192.168.2.104.2046 > 63.166.13.75.80: S 4045374969:4045374969(0) win
16384 <mss 1460,nop,nop,sackOK>"
```

note : all the sessions within are 1 second ; they are probably all related.

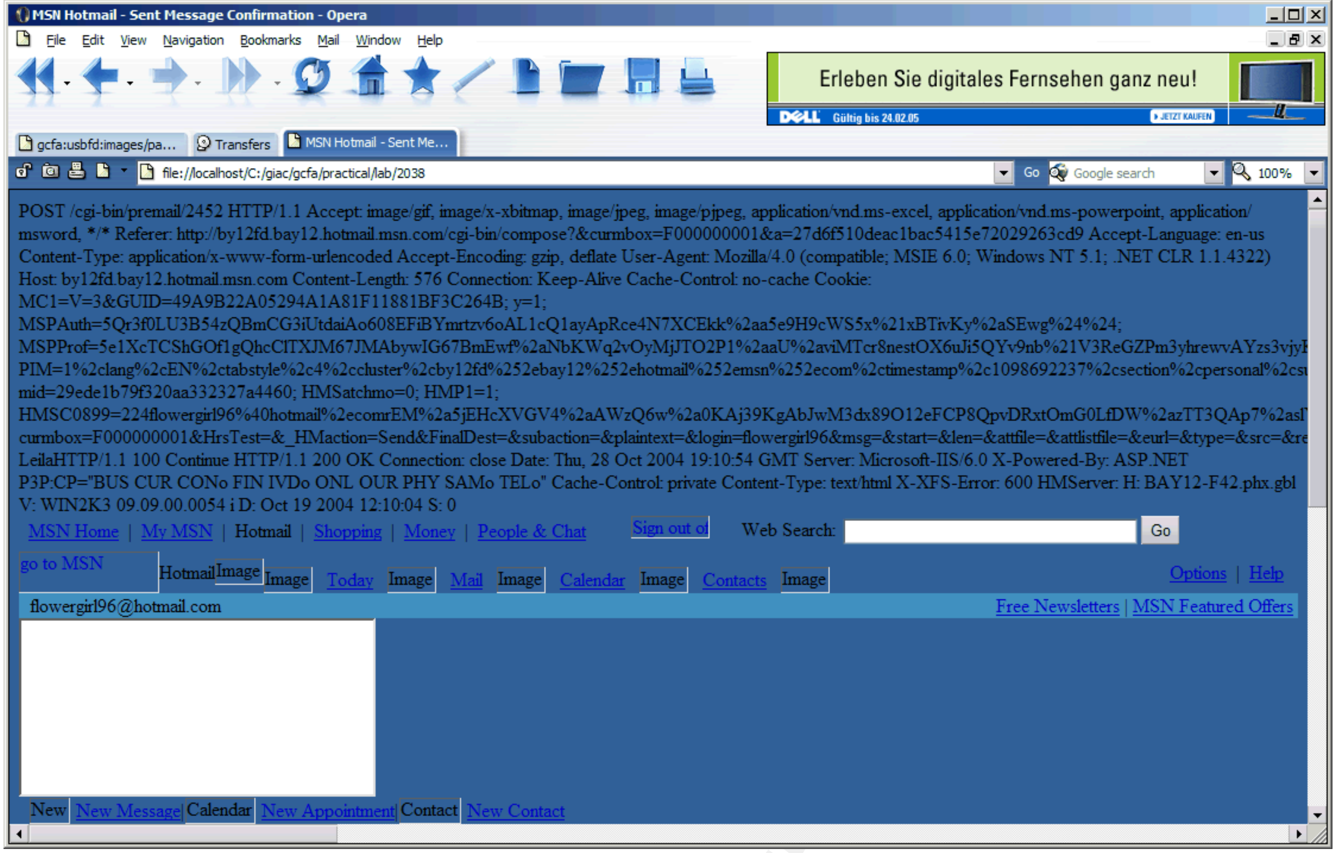
5.5.2 interesting sessions

I load them in ethereal and, for each session "analysis/follow tcp stream", saved in file, loaded in browser for more readability. Summary :

```
2038 : message sent by Leila Conlay to Sam..., meeting at a coffee shop
2039 : 3 x "ADSAdClient31.dll?GetAd?"etc :
2040 : idem
2041 : GET /c.gif2042 : GET /ads/363/0000000363_000000000000000112530.gif HTTP/1.1 2043 :
idem, images
2044 : session end immediately with reset
2045 : other site ; "Host: ad.doubleclick.net"
2046 : only Syn
```

5.5.3 The appointment

Only first the session (2038) interesting. Where is the rest of the communication ? probably


MSN Hotmail - Sent Message Confirmation - Opera
File Edit View Navigation Bookmarks Mail Window Help
Erleben Sie digitales Fernsehen ganz neu!
DELL Gültig bis 24.02.05
JETZT KAUFEN
gcfa:usbfd:images/pa...
Transfers
MSN Hotmail - Sent Me...
file://localhost/C:/giac/gcfa/practical/lab/2038
Go
Google search
100%

```
POST /cgi-bin/premail/2452 HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/
msword, */* Referer: http://by12fd.bay12.hotmail.msn.com/cgi-bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029263cd9 Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com Content-Length: 576 Connection: Keep-Alive Cache-Control: no-cache Cookie:
MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1;
MSPAuth=5Qr3f0LU3B54zQBmCG3iUtdaiAo608EFiBYmrtzv6oAL1cQ1ayApRce4N7XCEkk%2aa5e9H9cWS5x%21xBTivKy%2aSEwg%24%24;
MSPProf=5e1XcTCShGOf1gQhcClTXJM67JMAbywIG67BmEwf%2aNbKWq2vOyMjJTO2P1%2aaU%2aviMTcr8nestOX6uJi5QYv9nb%21V3ReGZPm3yhrewvAYzs3vjyl
PIM=1%2clang%2cEN%2ctabstyle%2c4%2ccluster%2cby12fd%252ebay12%252ehotmail%252emsn%252ecom%2ctimestamp%2c1098692237%2csection%2cpersonal%2cs
mid=29ede1b79f320aa332327a4460; HMSatchmo=0; HMP1=1;
HMSC0899=224flowergirl96%40hotmail%2ecomrEM%2a5jEHcXVGV4%2aAWzQ6w%2a0KAj39KgAbJwM3dx89O12eFCP8QpvDRxtOmG0LfDW%2azTT3QAp7%2as
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&r
LeilaHTTP/1.1 100 Continue HTTP/1.1 200 OK Connection: close Date: Thu, 28 Oct 2004 19:10:54 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" Cache-Control: private Content-Type: text/html X-XFS-Error: 600 HMServer: H: BAY12-F42.phx.gbl
V: WIN2K3 09.09.00.0054 i D: Oct 19 2004 12:10:04 S: 0
```

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat
Sign out of
Web Search:
Go
go to MSN
Hotmail Image
Image Today Image Mail Image Calendar Image Contacts Image
Options | Help
flowergirl96@hotmail.com
Free Newsletters | MSN Featured Offers
New New Message Calendar New Appointment Contact New Contact

cut for this practical. Here is an print screen of this session loaded in a browser and right after a summary of interesting data :

- This is the posting of an html form
- "Referer: http://by12fd.bay12.hotmail.msn.com/cgi-bin/compose ": this is hotmail (web based email)m
- "login=flowergirl96" : identification of the user
- to=SamGuarillo@hotmail.com : the recipient's email
- " subject=RE%3A+coffee " : subject of the email is "coffee"
- &body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm " : body of the message, meeting at the coffee shop on the corner Hollywood and McCadden ... at 7 PM
- " "HMSC0899=224flowergirl96%40hotmail%2ecom" : the sender is flowergirl96@hotmail.com2
- " LeilaHTTP/1.1 100 Continue" : reference to Leila Conlay, who is probably "flowergirl96"
- flowergirl96@hotmail.com : again
- "Your message has been sent to: "
- "SamGuarillo@hotmail.com"

Summary
Leila Conlay sends an email to SamGuarillo@hotmail.com ; appointment at a coffee shop.

5.6 What's next ?
Mr. Lawrence knows that the appointment is at " the coffee shop on the corner Hollywood and McCadden ... at 7 PM", he looks for a map of the place and shows up there at 7 PM. Right after, at 7 24 PM he prepares the "COFFEE.DOC" message.

6. Legal implications for Switzerland

Based on my findings the following SWISS law has been broken. (Note: as swiss laws are written in either french, german or italian, I will copy it in its original language and then try to translate it. Please consider that only the original text applies.)

5.1 Art. 143bis du code pénal (4)

> **Accès indu à un système informatique**
> Celui qui, sans dessein d'enrichissement, se sera introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part, sera, sur plainte, puni de l'emprisonnement ou de l'amende
>
> **Unauthorized access to a computer**
> Whoever, without the goal of gaining some wealth, gets access without proper authorization, with the mean of a data transmission unit, into a computer which belongs to somebody else, and, provided that the computer has been especially protected against access from him/her, he/she will be sent by prison or will have to pay a fine it he/she gets sued.

Discussion

Elements of the infraction:
Objective elements

- "***a computer which belongs to somebody else and it that computer has been especially protected against access from him***"
  - The system must belong to somebody else, which means that the author of the infraction can not access freely to this information. The system of Leila Conley does not belong to Mr. Lawrence, neither do the other network devices involved, or the hotmail server.
  - The system must be protected against access : Ms. Conley hotmail account is effectively protected by a password. I have not enough information to speak about the company's equipment which could have been subverted by Mr. Lawrence.
- "***access without proper authorization ... with the mean of a data transmission unit "***
  - ACCESS : this means enter a system with any mean, like a physical break-in. The installation of the sniffer can be considered here.
  - WITHOUT PROPER AUTHORIZATION : Mr. Lawrence had not the consent of miss Conley, neither from the system administration to use the sniffer.

Subjective elements

- ***Intention*** **:** Mr Lawrence knew what he was doing, he had not access to those data by accident.
- **"** ***without the goal of gaining some wealth***" : the objective of Mr. Lawrence was to gain

information about L.Conley private life. The article 143, which is similar, would apply if the goal were to gain some wealth.

The law applies only if Mr. Lawrence is sued. Prison can go up to 5 years.

5.2 Other articles

The "article 179 novies du Code Pénal" could be invoked too. It regards the "privacy" protection, but involves rather an unauthorized access to a file. In this case it is an email, so I do not think it applies.

5.3 Internal Acceptable Use Policy
Of course Mr. Lawrence might have broken a lot of internal rules, but as I am not aware of them they will not be considered here.

7. Recommandations for the follow-up action

7.1 Acceptable Use Policy
Most of the actions of mr. Lawrence should be prohibited by the AU policy. If it does not existe, write it down. It must contain the following points which apply directly to this case :

- Unacceptable use:
  - Harassing or threatening use
  - Network mapping or monitoring
  - Installing software : all software must be installed by system administrators
  - Any use in violation with the law
  - Use of unauthorized devices without specific authorization : users must not physically or electronically any device to company system or networks.

Make sure that the AU policy includes them, that it has been distributed, explained and understood by all users. You may organize presentations and illustrate them with real world example. What has just happened is a good start.

7.2 Do not give administrative rights to users unless it is necessary. This will make more difficult for them to install unauthorized software. With XP, do not include them in the "power users" group.

7.3 If possible prohibit the use of private email accounts during the business. The AU policy should make this clear. This will not prevent users from sending personal messages, but you will have the possibility to control it. Try to block access to sites like hotmail ; proxies can help.

7.4 In the same way restrict the usage of Internet for personal use. Systems should be used for business first.

8. Additional informations

- Précis de droit Staempfli, Bernard Corboz, "Les infractions en droit suisse, volume 1", Staempfli Editions SA Berne, for the legal implications in Switzerland

Annex

A1 Timeline

```
Mon Oct 25 2004 00:00:00    19968 .a. -/-rwxrwxrwx 0        0        3        E:\/her.doc
Mon Oct 25 2004 08:32:06    19968 ..c -/-rwxrwxrwx 0        0        3        E:\/her.doc
Mon Oct 25 2004 08:32:08    19968 m.. -/-rwxrwxrwx 0        0        3        E:\/her.doc
Tue Oct 26 2004 00:00:00    19968 .a. -/-rwxrwxrwx 0        0        4        E:\/hey.doc
Tue Oct 26 2004 08:48:06    19968 ..c -/-rwxrwxrwx 0        0        4        E:\/hey.doc
Tue Oct 26 2004 08:48:10    19968 m.. -/-rwxrwxrwx 0        0        4        E:\/hey.doc
Wed Oct 27 2004 00:00:00   450560 .a. -/-rwxrwxrwx 0        0        12       E:\/WinDump.exe
(_INDUMP.EXE) (deleted)
                           485810 .a. -/-rwxrwxrwx 0        0        7
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                                0 .a. -rwxrwxrwx 0        0        7        <part1.dd-_INPCA~1.EXE-dead-
7>
                                0 .a. -rwxrwxrwx 0        0        12       <part1.dd-_INDUMP.EXE-dead-
12>
Wed Oct 27 2004 16:23:50   485810 m.. -/-rwxrwxrwx 0        0        10
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                           485810 m.. -rwxrwxrwx 0        0        10       <part1.dd-_INPCA~1.EXE-dead-
10>
Wed Oct 27 2004 16:23:54        0 ..c -rwxrwxrwx 0        0        7        <part1.dd-_INPCA~1.EXE-dead-
7>
                           485810 ..c -rwxrwxrwx 0        0        10       <part1.dd-_INPCA~1.EXE-dead-
10>
                           485810 ..c -/-rwxrwxrwx 0        0        7
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
                           485810 ..c -/-rwxrwxrwx 0        0        10
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:56        0 m.. -rwxrwxrwx 0        0        7        <part1.dd-_INPCA~1.EXE-dead-
7>
                           485810 m.. -/-rwxrwxrwx 0        0        7
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:24:02   450560 m.. -rwxrwxrwx 0        0        14       <part1.dd-_INDUMP.EXE-dead-
14>
                           450560 m.. -/-rwxrwxrwx 0        0        14       E:\/WinDump.exe
(_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04   450560 ..c -/-rwxrwxrwx 0        0        12       E:\/WinDump.exe
(_INDUMP.EXE) (deleted)
                           450560 ..c -/-rwxrwxrwx 0        0        14       E:\/WinDump.exe

(_INDUMP.EXE) (deleted)
                                0 ..c -rwxrwxrwx 0        0        12       <part1.dd-_INDUMP.EXE-dead-
12>
                           450560 ..c -rwxrwxrwx 0        0        14       <part1.dd-_INDUMP.EXE-dead-
14>
Wed Oct 27 2004 16:24:06        0 m.. -rwxrwxrwx 0        0        12       <part1.dd-_INDUMP.EXE-dead-
12>
                           450560 m.. -/-rwxrwxrwx 0        0        12       E:\/WinDump.exe
(_INDUMP.EXE) (deleted)
Thu Oct 28 2004 00:00:00   485810 .a. -rwxrwxrwx 0        0        10       <part1.dd-_INPCA~1.EXE-dead-
10>
                             8814 .a. -rwxrwxrwx 0        0        17       <part1.dd-_ap.gif-dead-17>
                           450560 .a. -rwxrwxrwx 0        0        14       <part1.dd-_INDUMP.EXE-dead-
14>
                           450560 .a. -/-rwxrwxrwx 0        0        14       E:\/WinDump.exe

(_INDUMP.EXE) (deleted)
                                0 .a. -rwxrwxrwx 0        0        16       <part1.dd-_ap.gif-dead-16>
                            53056 .a. -/-rwxrwxrwx 0        0        15       E:\/_apture (deleted)
                            53056 .a. -rwxrwxrwx 0        0        15       <part1.dd-_apture-dead-15>
                            19968 .a. -/-rwxrwxrwx 0        0        18       E:\/coffee.doc
                             8814 .a. -/-rwxrwxrwx 0        0        17       E:\/_ap.gif (deleted)
                             8814 .a. -/-rwxrwxrwx 0        0        16       E:\/_ap.gif (deleted)
                           485810 .a. -/-rwxrwxrwx 0        0        10
E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Thu Oct 28 2004 11:08:24    53056 ..c -/-rwxrwxrwx 0        0        15       E:\/_apture (deleted)
                            53056 ..c -rwxrwxrwx 0        0        15       <part1.dd-_apture-dead-15>
Thu Oct 28 2004 11:11:00    53056 m.. -/-rwxrwxrwx 0        0        15       E:\/_apture (deleted)
                            53056 m.. -rwxrwxrwx 0        0        15       <part1.dd-_apture-dead-15>
Thu Oct 28 2004 11:17:44     8814 ..c -/-rwxrwxrwx 0        0        16       E:\/_ap.gif (deleted)
                                0 ..c -rwxrwxrwx 0        0        16       <part1.dd-_ap.gif-dead-16>
                             8814 ..c -/-rwxrwxrwx 0        0        17       E:\/_ap.gif (deleted)
                             8814 ..c -rwxrwxrwx 0        0        17       <part1.dd-_ap.gif-dead-17>
Thu Oct 28 2004 11:17:46     8814 m.. -/-rwxrwxrwx 0        0        17       E:\/_ap.gif (deleted)
                                0 m.. -rwxrwxrwx 0        0        16       <part1.dd-_ap.gif-dead-16>
                             8814 m.. -/-rwxrwxrwx 0        0        16       E:\/_ap.gif (deleted)
                             8814 m.. -rwxrwxrwx 0        0        17       <part1.dd-_ap.gif-dead-17>
Thu Oct 28 2004 19:24:46    19968 ..c -/-rwxrwxrwx 0        0        18       E:\/coffee.doc
Thu Oct 28 2004 19:24:48    19968 m.. -/-rwxrwxrwx 0        0        18       E:\/coffee.doc
```

9. List of references

(1) Windump, the port of "tcpdump" to Windows : http://windump.polito.it/
(2) Analysis of network traffic in covered in depth in track 3 of Sans courses " Intrusion Detection In-Depth" : http://www.sans.org. I found some helpful hints to analyze tcpdump capture files in both :
(2a) Pete Storm GCIA practical
http://www.giac.org/certified_professionals/practicals/gcia/0678.php
(2b) Sylvain Randier GCIA practical
http://www.giac.org/certified_professionals/practicals/gcia/0620.php
(3) P0f, a versatile passive OS fingerprinting tool, http://lcamtuf.coredump.cx/p0f.shtml
(4) Article 143bis du Code pénal suisse : http://www.admin.ch/ch/f/rs/311_0/a143bis.html