1 . What are the hash values (MD5 & SHA-1) of all images?

```
[leviathan3773@latitude:DDs ] $ md5sum cfreds_2015_data_leakage_pc.dd && sha1sum
 cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde  cfreds_2015_data_leakage_pc.dd
afe5c9ab487bd47a8a9856b1371c2384d44fd785  cfreds_2015_data_leakage_pc.dd

[leviathan3773@latitude:DDs ] $ md5sum cfreds_2015_data_leakage_rm#2.dd && sha1s
um cfreds_2015_data_leakage_rm#2.dd
b4644902acab4583a1d0f9f1a08faa77  cfreds_2015_data_leakage_rm#2.dd
048961a85ca3eced8cc73f1517442d31d4dca0a3  cfreds_2015_data_leakage_rm#2.dd

[leviathan3773@latitude:DDs ] $ md5sum cfreds_2015_data_leakage_rm#3_type2.dd &&
 sha1sum cfreds_2015_data_leakage_rm#3_type2.dd
858c7250183a44dd83eb706f3f178990  cfreds_2015_data_leakage_rm#3_type2.dd
471d3eedca9add872fc0708297284e1960ff44f8  cfreds_2015_data_leakage_rm#3_type2.dd
[leviathan3773@latitude:DDs ] $
```

2 . Does the acquisition and verification hash value match?
No

3 . Identify the partition information of PC image.

```
Disk /dev/loop0: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0265720

Disk /dev/loop1: 20 GiB, 21474836480 bytes, 41943040 sectors
/dev/loop1p1 *        2048   206847   204800  100M  7 HPFS/NTFS/exFAT
/dev/loop1p2        206848 41940991 41734144 19,9G  7 HPFS/NTFS/exFAT
```

4 . Explain installed OS information in detail.
        (OS name, install date, registered owner…)

Know OS name:

```
        (C:\Windows\System32\ñicense.rtf)
        $> cd /mnt/windows/pc2/Windows/System32
        $> find ./ -name 'license.*'
        $> grep "[Ww]indows [0-9]" license.rtf
```

Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

```
\Microsoft\Windows NT\CurrentVersion> cat CurrentVersion
Value <CurrentVersion> of type REG_SZ (1), data length 8 [0x8]
6.1

\Microsoft\Windows NT\CurrentVersion> cat EditionID
Value <EditionID> of type REG_SZ (1), data length 18 [0x12]
Ultimate

Microsoft\Windows NT\CurrentVersion> cat SystemRoot
Value <SystemRoot> of type REG_SZ (1), data length 22 [0x16]
C:\Windows

\Microsoft\Windows NT\CurrentVersion> cat ProductName
Value <ProductName> of type REG_SZ (1), data length 38 [0x26]
```

```
Windows 7 Ultimate

\Microsoft\Windows NT\CurrentVersion> cat CurrentBuildNumber
Value <CurrentBuildNumber> of type REG_SZ (1), data length 10 [0xa]
7601
```

The process of compiling and packaging an application is sometimes referred to as "building". A version such as 10.3.5 will be compiled many times before it is released. Each of these "builds" are numbered so developers can keep track of changes and problems. Think of it as versions of the released version

Os system

```
Windows 7 Ultimate 6.1 7601
```

Installation date *

```
  size     type              value name             [value if type DWORD]
     8  1 REG_SZ             <CurrentVersion>
    10  1 REG_SZ             <CurrentBuild>
    14  1 REG_SZ             <SoftwareType>
    40  1 REG_SZ             <CurrentType>
     4  4 REG_DWORD          <InstallDate>     1427034866 [0x550ed2f2]*
     2  1 REG_SZ             <RegisteredOrganization>
    20  1 REG_SZ             <RegisteredOwner>
    22  1 REG_SZ             <SystemRoot>
    14  1 REG_SZ             <InstallationType>
    18  1 REG_SZ             <EditionID>
    38  1 REG_SZ             <ProductName>
    48  1 REG_SZ             <ProductId>
   164  3 REG_BINARY         <DigitalProductId>
  1272  3 REG_BINARY         <DigitalProductId4>
    10  1 REG_SZ             <CurrentBuildNumber>
    58  1 REG_SZ             <BuildLab>
    88  1 REG_SZ             <BuildLabEx>
    74  1 REG_SZ             <BuildGUID>
    10  1 REG_SZ             <CSDBuildNumber>
    22  1 REG_SZ             <PathName>
    30  1 REG_SZ             <CSDVersion>

\Microsoft\Windows NT\CurrentVersion>


[leviathan3773@latitude:~ ] $ date -d @1427034866
dom mar 22 15:34:26 CET 2015
[leviathan3773@latitude:~ ] $ echo 1427034866 | gawk '{print strftime("%c",$0)}'
dom 22 mar 2015 15:34:26 CET
```

Dueño del registro

```
\Microsoft\Windows NT\CurrentVersion> cat RegisteredOwner
Value <RegisteredOwner> of type REG_SZ (1), data length 20 [0x14]
informant
```

6 . What is the timezone setting?

```
\ControlSet001\Control> cd TimeZoneInformation

\ControlSet001\Control\TimeZoneInformation> ls
Node has 0 subkeys and 10 values
  size     type              value name             [value if type DWORD]
     4  4 REG_DWORD          <Bias>                   300 [0x12c]
     4  4 REG_DWORD          <DaylightBias>           -60 [0xffffffc4]
    32  1 REG_SZ             <DaylightName>
    16  3 REG_BINARY         <DaylightStart>
     4  4 REG_DWORD          <StandardBias>             0 [0x0]
    32  1 REG_SZ             <StandardName>
    16  3 REG_BINARY         <StandardStart>
   256  1 REG_SZ             <TimeZoneKeyName>
     4  4 REG_DWORD          <DynamicDaylightTimeDisabled> 0  [0x0]
     4  4 REG_DWORD          <ActiveTimeBias>         240 [0xf0]

\ControlSet001\Control\TimeZoneInformation>

\ControlSet001\Control\TimeZoneInformation> cat TimeZoneKeyName
Value <TimeZoneKeyName> of type REG_SZ (1), data length 256 [0x100]
Eastern Standard Time

[Timezone] Eastern Northamerica
-------------------------------
```

==

North America
U.S. states using EST in the winter and EDT in the summer:

Connecticut
Delaware
District of Columbia
Florida - Southern/Eastern parts Show
Georgia
Indiana - all except for these north-western counties near Chicago (Lake, Porter,
La Porte, Newton, Jasper, Starke) and these south-western counties in Indiana near Evansville Show
Kentucky - eastern parts Show
Maine
Maryland
Massachusetts
Michigan - most except these western counties Show
New Hampshire
New Jersey
New York
North Carolina
Ohio
Pennsylvania
Rhode Island
South Carolina
Tennessee - eastern counties Show
Vermont
Virginia
West Virginia

Canadian provinces/territories using EST in the winter and EDT in the summer:

Nunavut - most of it Show
Ontario - most parts east of 90 West and two communities west of 90 West Show
Quebec - most of it Show

Canadian provinces/territories using EST all year:

Nunavut - Southampton Island only (Coral Harbour)

Mexican states using EST all year:

Quintana Roo

Caribbean
Caribbean countries using EST in the winter and EDT in the summer:

Bahamas
Haiti

Caribbean countries using EST all year:

Jamaica

Central America
Central American countries using EST all year:

Panama

```
================================================================================
=================================
```

Crack passwords from registries

```
[leviathan3773@latitude:Descargas ] $ bkhive /mnt/windows/hdd/Windows/System32/c
onfig/SYSTEM /tmp/saved-syskey.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}
Default ControlSet: 001
Bootkey: face85b8f08c42ca889ee83551ee1e6f

[leviathan3773@latitude:Descargas ] $ samdump2 /mnt/windows/hdd/Windows/System32
/config/SAM /tmp/saved-syskey.txt > /tmp/hashes.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}
[leviathan3773@latitude:Descargas ] $ cat /tmp/hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
informant:1000:aad3b435b51404eeaad3b435b51404ee:9e3d31b073e60bfd7b07978d6f914d0a
:::
admin11:1001:aad3b435b51404eeaad3b435b51404ee:21759544b2d7efccc978449463cf7e63::
:
ITechTeam:1002:aad3b435b51404eeaad3b435b51404ee:75ed0cb7676889ab43764a3b7d3e6943
```

```
:::
temporary:1003:aad3b435b51404eeaad3b435b51404ee:1b3801b608a6be89d21fd3c5729d30bf
:::
[leviathan3773@latitude:Descargas ] $
```

Crack them

```
31d6cfe0d16ae931b73c59d7e0c089c0 [Not found]
31d6cfe0d16ae931b73c59d7e0c089c0 [Not found]
9e3d31b073e60bfd7b07978d6f914d0a [Not found]
21759544b2d7efccc978449463cf7e63 NTLM : djemals11
75ed0cb7676889ab43764a3b7d3e6943 [Not found]
1b3801b608a6be89d21fd3c5729d30bf NTLM : xpavhfkfl
```

7 . What is the computer name?

```
(...)\Control\ComputerName\ComputerName> cat ComputerName

Value <ComputerName> of type REG_SZ (1), data length 26 [0x1a]


INFORMANT-PC
```

8 . List all accounts in OS except the system accounts: Administrator, Guest, systemprofile, LocalService, NetworkService.
(Account name, login count, last logon date…)

En el registro [SAM] (Security Account Manager)

```
\SAM\Domains\Account\Users\Names> ls
Node has 6 subkeys and 1 values
  key name
  <admin11>
  <Administrator>
  <Guest>
  <informant>
  <ITechTeam>
  <temporary>
  size     type              value name             [value if type DWORD]
     0  0 REG_NONE           <>

\SAM\Domains\Account\Users\Names>

\SAM\Domains\Account\Users> ls
Node has 7 subkeys and 1 values
  key name
  <000001F4>
  <000001F5>
  <000003E8>
  <000003E9>
  <000003EA>
  <000003EB>
  <Names>
  size     type              value name             [value if type DWORD]
     0  6 REG_LINK           <>

\SAM\Domains\Account\Users>


(...)\Windows NT\CurrentVersion\ProfileList> ls
Node has 6 subkeys and 4 values
```

```
  key name
  <S-1-5-18>
  <S-1-5-19>
  <S-1-5-20>
  <S-1-5-21-2425377081-3129163575-2985601102-1000>
  <S-1-5-21-2425377081-3129163575-2985601102-1001>
  <S-1-5-21-2425377081-3129163575-2985601102-1003>
  size     type              value name             [value if type DWORD]
    40  2 REG_EXPAND_SZ      <ProfilesDirectory>
    56  2 REG_EXPAND_SZ      <Default>
    54  2 REG_EXPAND_SZ      <Public>
    52  2 REG_EXPAND_SZ      <ProgramData>

(...)\Windows NT\CurrentVersion\ProfileList>
```

Default: It's the value whose name is null.

Flags: enable you to control the installation and uninstallation of your registry entries.

ProfileImagePath: The User profiles` path.

ProfileLoadTimeHigh: Profile load time of user

ProfileLoadTimeLow: Profile load time low of user

RefCount: `0` value means the account has no active session, not `0`value means the account has an active session.

Sid:Security Identifier.

State: indicates the state of the local profile cache.

0001	Profile is mandatory.
0002	Update the locally cached profile.
0004	New local profile.
0008	New central profile.
0010	Update the central profile.
0020	Delete the cached profile.
0040	Upgrade the profile.
0080	Using Guest user profile.
0100	Using Administrator profile.
0200	Default net profile is available and ready.
0400	Slow network link identified.
0800	Temporary profile loaded.

RunLogonScriptSync : Determines whether the system waits for the logon script to finish running before it starts Windows Explorer and creates the desktop.

0	The logon script and Windows Explorer can run simultaneously.
1	Windows Explorer does not start until the logon script has finished running.

Información útil

```
(...)\Windows NT\CurrentVersion\ProfileList> cd S-1-5-21-2425377081-3129163575-2985601102-1000

(...)> ls
Node has 0 subkeys and 8 values
```

```
  size     type              value name             [value if type DWORD]
    38  2 REG_EXPAND_SZ      <ProfileImagePath>
     4  4 REG_DWORD          <Flags>                     0 [0x0]
     4  4 REG_DWORD          <State>                     0 [0x0]
    28  3 REG_BINARY         <Sid>
     4  4 REG_DWORD          <ProfileLoadTimeLow>        0 [0x0]
     4  4 REG_DWORD          <ProfileLoadTimeHigh>       0 [0x0]
     4  4 REG_DWORD          <RefCount>                  0 [0x0]
     4  4 REG_DWORD          <RunLogonScriptSync>        0 [0x0]

(...)> cat ProfileImagePath
Value <ProfileImagePath> of type REG_EXPAND_SZ (2), data length 38 [0x26]
C:\Users\informant


(...)>
```

```
Usuario [informant]:

    · <ProfileImagePath> = C:\Users\informant
    · <Flags> = 0x00000000
    · <State> = 0x00000000
    · <Sid>
      Value <Sid> of type REG_BINARY (3), data length 28 [0x1c]
      :00000  01 05 00 00 00 00 00 05 15 00 00 00 39 51 90 90 ............9Q..
      :00010  37 3F 83 BA 4E A8 F4 B1 E8 03 00 00             7?..N.......

    · <ProfileLoadTimeLow>  = 0x00000000
    · <ProfileLoadTimeHigh> = 0x00000000
    · <RefCount> = 0x00000000
    · <RunLogonScriptSync> = 0x00000000
```

Explicación de los campos del registro [SAM\Domains\Account\Users\*]

===

The {RID}, or Relative Identifier, is the portion of a Security Identifier (SID) that identifies a user or group in relation to the authority that issued the SID. Besides providing quite a bit of information about how SIDs are created, Microsoft also provides a list of RIDs (http://support.microsoft.com/kb/157234)
for well-known users and groups as well as well-known aliases (seen in the SAM\SAM\Domains\Builtin\Aliases key).

The F value within the key is a binary data type and must be parsed appropriately
(see the sam.h file, part of the source code for Peter’s utility) to extract all

the information. Some important dates are available in the contents of the binary
data for the F value—specifically, several time/date stamps represented as 64-bit
FILETIME objects. Those values and their locations are as follows:

■ Bytes 8-15 represent the last login date for the account.

■ Bytes 24-31 represent the date that the password was last reset
(if the password hasn’t been reset or changed, this date will correlate to the account creation date).

- Bytes 32-39 represent the account expiration date.

- Bytes 40-47 represent the date of the last failed login attempt (because the account name has to be correct for the date to be changed on a specific account, this date can also be referred to as the date of the last incorrect password usage).

```
================================================================================
=================================

Access date
-----------

[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Windows/Sy
stem32/config/SAM -f sam
Parsed Plugins file.
Launching samparse v.20160203
samparse v.20160203
(SAM) Parse SAM file for user & group mbrshp info


User Information
-------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
Login Count     : 6
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password not required
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : informant [1000]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 14:33:54 2015 Z
Name            :
Password Hint   : IAMAN
```

```
Last Login Date : Wed Mar 25 14:45:59 2015 Z
Pwd Reset Date  : Sun Mar 22 14:33:54 2015 Z
Pwd Fail Date   : Wed Mar 25 14:45:43 2015 Z
Login Count     : 10
  --> Password not required
  --> Password does not expire
  --> Normal user account

Username        : admin11 [1001]
Full Name       : admin11
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:51:54 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date  : Sun Mar 22 15:52:10 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 2
  --> Password does not expire
  --> Normal user account

Username        : ITechTeam [1002]
Full Name       : ITechTeam
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:52:30 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Sun Mar 22 15:52:45 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : temporary [1003]
Full Name       : temporary
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Sun Mar 22 15:53:01 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:55:57 2015 Z
Pwd Reset Date  : Sun Mar 22 15:53:11 2015 Z
Pwd Fail Date   : Sun Mar 22 15:56:37 2015 Z
Login Count     : 1
  --> Password does not expire
  --> Normal user account

...
```

9 . Who was the last user to logon into PC?

Último usuario que ha iniciado sesión

```
(...)\CurrentVersion\Authentication\LogonUI> cat LastLoggedOnSAMUser
Value <LastLoggedOnSAMUser> of type REG_SZ (1), data length 46 [0x2e]
informant-PC\informant


(...)\CurrentVersion\Authentication\LogonUI> cat LastLoggedOnUser
```

```
Value <LastLoggedOnUser> of type REG_SZ (1), data length 24 [0x18]
.\informant


(...)\CurrentVersion\Authentication\LogonUI>
```

10 . When was the last recorded shutdown date/time?

```
\ControlSet001\Control\Windows> ls
Node has 0 subkeys and 10 values
  size     type              value name             [value if type DWORD]
     4  4 REG_DWORD          <ErrorMode>                 0 [0x0]
    26  2 REG_EXPAND_SZ      <Directory>
     4  4 REG_DWORD          <NoInteractiveServices>     0 [0x0]
    44  2 REG_EXPAND_SZ      <SystemDirectory>
     4  4 REG_DWORD          <ShellErrorMode>            1 [0x1]
     4  4 REG_DWORD          <CSDVersion>              256 [0x100]
     4  4 REG_DWORD          <CSDReleaseType>            0 [0x0]
     4  4 REG_DWORD          <CSDBuildNumber>        17514 [0x446a]
     4  4 REG_DWORD          <ComponentizedBuild>        1 [0x1]
     8  3 REG_BINARY         <ShutdownTime>

\ControlSet001\Control\Windows> cat ShutdownTime
Value <ShutdownTime> of type REG_BINARY (3), data length 8 [0x8]
:00000  57 A9 48 B5 10 67 D0 01                         W.H..g..


\ControlSet001\Control\Windows>

[leviathan3773@latitude:Escritorio ] $ cat regBinaryshutdownTime.py
#! /usr/bin/python3

from __future__ import division
import struct
import sys
from binascii import unhexlify
from datetime import datetime, timedelta

nt_timestamp = struct.unpack("<Q", unhexlify(sys.argv[1]))[0]
epoch = datetime(1601, 1, 1, 0, 0, 0)
nt_datetime = epoch + timedelta(microseconds=nt_timestamp / 10)

print(nt_datetime.strftime("%c"))
[leviathan3773@latitude:Escritorio ] $ python3 regBinaryshutdownTime.py 57A948B5
1067D001
Wed Mar 25 15:31:05 2015
[leviathan3773@latitude:Escritorio ] $
```

11 . Explain the information of network interface(s) with an IP address assigned by DHCP.

```
------------------------------------------------------------------------
[leviathan3773@latitude:config ] $ chntpw -e SOFTWARE

(...)\Windows NT\CurrentVersion\NetworkCards\8> ls
Node has 0 subkeys and 2 values
  size     type              value name             [value if type DWORD]
    78  1 REG_SZ             <ServiceName>
    80  1 REG_SZ             <Description>

(...)\Windows NT\CurrentVersion\NetworkCards\8> cat ServiceName
Value <ServiceName> of type REG_SZ (1), data length 78 [0x4e]
{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}


(...)\Windows NT\CurrentVersion\NetworkCards\8> cat Description
Value <Description> of type REG_SZ (1), data length 80 [0x50]
Intel(R) PRO/1000 MT Network Connection


(...)\Windows NT\CurrentVersion\NetworkCards\8>
------------------------------------------------------------------------

In HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfa
ces\\
{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}

Relevant information
--------------------

(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> ls
Node has 0 subkeys and 25 values
  size     type              value name             [value if type DWORD]
     4  4 REG_DWORD          <UseZeroBroadcast>         0 [0x0]
     4  4 REG_DWORD          <EnableDeadGWDetect>       1 [0x1]
     4  4 REG_DWORD          <EnableDHCP>               1 [0x1]
     2  1 REG_SZ             <NameServer>
     2  1 REG_SZ             <Domain>
     4  4 REG_DWORD          <RegistrationEnabled>      1 [0x1]
     4  4 REG_DWORD          <RegisterAdapterName>      0 [0x0]
    26  1 REG_SZ             <DhcpIPAddress>
    28  1 REG_SZ             <DhcpSubnetMask>
    26  1 REG_SZ             <DhcpServer>
     4  4 REG_DWORD          <Lease>                 1800 [0x708]
     4  4 REG_DWORD          <LeaseObtainedTime> 1427296790 [0x5512d216]
     4  4 REG_DWORD          <T1>              1427297690 [0x5512d59a]
     4  4 REG_DWORD          <T2>              1427298365 [0x5512d83d]
     4  4 REG_DWORD          <LeaseTerminatesTime> 1427298590 [0x5512d91e]
     4  4 REG_DWORD          <AddressType>              0 [0x0]
     4  4 REG_DWORD          <IsServerNapAware>         0 [0x0]
     4  4 REG_DWORD          <DhcpConnForceBroadcastFlag> 0 [0x0]
   220  3 REG_BINARY         <DhcpInterfaceOptions>
    14  3 REG_BINARY         <DhcpGatewayHardware>
     4  4 REG_DWORD          <DhcpGatewayHardwareCount> 1 [0x1]
    22  1 REG_SZ             <DhcpNameServer>
    24  7 REG_MULTI_SZ       <DhcpDefaultGateway>
    24  1 REG_SZ             <DhcpDomain>
    30  7 REG_MULTI_SZ       <DhcpSubnetMaskOpt>



(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpIPAddress
Value <DhcpIPAddress> of type REG_SZ (1), data length 26 [0x1a]
10.11.11.129

(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpSubnetMask
Value <DhcpSubnetMask> of type REG_SZ (1), data length 28 [0x1c]
255.255.255.0
```

```
(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpServer
Value <DhcpServer> of type REG_SZ (1), data length 26 [0x1a]
10.11.11.254

(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpNameServer
Value <DhcpNameServer> of type REG_SZ (1), data length 22 [0x16]
10.11.11.2


(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpDefaultGateway
Value <DhcpDefaultGateway> of type REG_MULTI_SZ (7), data length 24 [0x18]
10.11.11.2



(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpDomain
Value <DhcpDomain> of type REG_SZ (1), data length 24 [0x18]
localdomain

(...)\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}> cat DhcpSubnetMaskOpt
Value <DhcpSubnetMaskOpt> of type REG_MULTI_SZ (7), data length 30 [0x1e]
255.255.255.0
```

Parameters explication -> [https://technet.microsoft.com/en-us/library/cc959606.aspx]

UseZeroBroadcast
Clave: Tcpip\Parameters\Interfaces\Id. de adaptador
Tipo del valor: REG_DWORD (booleano)
Intervalo válido: 0 o 1 (falso o verdadero)
Valor predeterminado: 0 (falso)
Descripción: si este parámetro se establece en 1 (verdadero), IP utilizará difusiones de ceros (0.0.0.0) en lugar de difusiones de unos (255.255.255.255). La mayoría de los equipos utilizan difusiones de unos, pero ciertos equipos derivados de implementaciones BSD utilizan difusiones de ceros. Los equipos que utilizan difusiones diferentes no interactúan bien en una misma red.

...

12 . What applications were installed by the suspect after installing OS?

Compare with:

```
----------------------------------------------------
[leviathan3773@latitude:Default ] $ pwd
/mnt/windows/hdd/Users/Default
[leviathan3773@latitude:Default ] $ cd Application\ Data
[leviathan3773@latitude:Application Data ] $ ls
Media Center Programs  Microsoft
[leviathan3773@latitude:Application Data ] $ cd Microsoft/
[leviathan3773@latitude:Microsoft ] $ ls
Internet Explorer  Windows
[leviathan3773@latitude:Microsoft ] $
----------------------------------------------------
```

```
[leviathan3773@latitude:Application Data ] $ ls -la
total 12
drwxrwxrwx 1 root root 4096 mar 23  2015 .
drwxrwxrwx 1 root root    0 mar 23  2015 ..
drwxrwxrwx 1 root root    0 mar 22  2015 Adobe
drwxrwxrwx 1 root root 4096 mar 25  2015 Apple Computer
drwxrwxrwx 1 root root    0 mar 22  2015 Identities
drwxrwxrwx 1 root root    0 nov 21  2010 Media Center Programs
drwxrwxrwx 1 root root 4096 mar 24  2015 Microsoft
[leviathan3773@latitude:Application Data ] $
```

```
[leviathan3773@latitude:Microsoft ] $ ls -la
total 16
drwxrwxrwx 1 root root 4096 mar 24  2015 .
drwxrwxrwx 1 root root 4096 mar 23  2015 ..
drwxrwxrwx 1 root root    0 mar 22  2015 AddIns
drwxrwxrwx 1 root root    0 mar 23  2015 Bibliography
drwxrwxrwx 1 root root    0 mar 22  2015 Credentials
drwxrwxrwx 1 root root    0 mar 22  2015 Crypto
drwxrwxrwx 1 root root    0 mar 23  2015 Document Building Blocks
drwxrwxrwx 1 root root    0 mar 24  2015 Excel
drwxrwxrwx 1 root root    0 mar 22  2015 Internet Explorer
drwxrwxrwx 1 root root    0 mar 22  2015 Network
drwxrwxrwx 1 root root    0 mar 23  2015 Office
drwxrwxrwx 1 root root    0 mar 22  2015 Outlook
drwxrwxrwx 1 root root    0 mar 23  2015 PowerPoint
drwxrwxrwx 1 root root    0 mar 23  2015 Proof
drwxrwxrwx 1 root root    0 mar 22  2015 Protect
drwxrwxrwx 1 root root    0 mar 24  2015 Sticky Notes
drwxrwxrwx 1 root root    0 mar 22  2015 SystemCertificates
drwxrwxrwx 1 root root 4096 mar 25  2015 Templates
drwxrwxrwx 1 root root    0 mar 23  2015 UProof
drwxrwxrwx 1 root root 4096 mar 23  2015 Windows
drwxrwxrwx 1 root root    0 mar 24  2015 Word
[leviathan3773@latitude:Microsoft ] $
```

Consideration...

```
------------------------------------------------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninsta
ll
HKEY_CURRENT_USER\Software\Microsoft\Installer\Products
------------------------------------------------------------------------
```

In [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~]

```
------------------------------------------------------------------------
(...)\{C6E287F1-2E47-45F0-BB51-94F815CFFB48}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 36 [0x24]
Eraser 6.2.0.2962

(...)\{C6E287F1-2E47-45F0-BB51-94F815CFFB48}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150325

--------------------------------------------------------------
```

Eraser is an advanced security tool for Windows which allows
you to completely remove sensitive data from your hard drive
by overwriting it several times with carefully selected

```
patterns. Eraser is currently supported under Windows XP
(with Service Pack 3), Windows Server 2003 (with Service Pack
2), Windows Vista, Windows Server 2008, Windows 7,8 ,10 and
Windows Server 2012.
-------------------------------------------------------------

(...)\{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 84 [0x54]
Microsoft .NET Framework 4 Client Profile


(...)\{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150325

(...)\{8E34682C-8118-31F1-BC4C-98CD9675E1C2}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 72 [0x48]
Microsoft .NET Framework 4 Extended


(...)\{8E34682C-8118-31F1-BC4C-98CD9675E1C2}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150325

(...)\{8E34682C-8118-31F1-BC4C-98CD9675E1C2}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 72 [0x48]
Microsoft .NET Framework 4 Extended


(...)\{8E34682C-8118-31F1-BC4C-98CD9675E1C2}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150325
-----------------------------------------------------------------------


In [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uni
nstall]:
--------------------------------------------------------------------------------
-------

(...)\{6C36881B-0E51-4231-9D02-BF2149664D34}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 26 [0x1a]
Google Drive


(...)\{6C36881B-0E51-4231-9D02-BF2149664D34}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150323

(...)\{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 42 [0x2a]
Google Update Helper


(...)\{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150322

(...)\{78002155-F025-4070-85B3-7C0453561701}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 52 [0x34]
```

```
Apple Application Support


(...)\{78002155-F025-4070-85B3-7C0453561701}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150323

(...)\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}> cat DisplayName
Value <DisplayName> of type REG_SZ (1), data length 44 [0x2c]
Apple Software Update


(...)\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}> cat InstallDate
Value <InstallDate> of type REG_SZ (1), data length 18 [0x12]
20150323
```

Powershell

```
Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* \
| Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table –AutoSize
```

Solution

Information relevant to specific users of the system is located in the ‘NTUSER.DAT’ file.

In [/mnt/windows/hdd/Users/informant/NTUSET.DAT]
(HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components>)

```
$> chntpw -e NTUSER.DAT
```

13 . List application execution logs.
(Executable path, execution time, execution count...)

Several Registry Keys store information about programs that have been executed previously on the system:

```
HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store
```

To open them tap on the Windows-key, type regedit and hit enter. This should open the
Windows Registry editor. You may receive a UAC (User Account Control) prompt which you need to accept.

```
--------------------------------------------------------------------------------
---------------------------------


HKU\informant\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compat
ibility Assistant
********************************************************************************
*****************

(...)\Compatibility Assistant\Persisted> ls
Node has 0 subkeys and 5 values
  size     type              value name             [value if type DWORD]
     4  4 REG_DWORD          <C:\Users\informant\Desktop\Download\IE11-Windows6.
1-x64-en-us.exe> 1                                        [0x1]
     4  4 REG_DWORD          <C:\Users\informant\Downloads\icloudsetup.exe> 1
                [0x1]
     4  4 REG_DWORD          <C:\Users\informant\Downloads\googledrivesync.exe>
1                       [0x1]
     4  4 REG_DWORD          <C:\Users\informant\Desktop\Download\Eraser 6.2.0.2
962.exe> 1                                [0x1]
     4  4 REG_DWORD          <C:\Users\informant\Desktop\Download\ccsetup504.exe
> 1                         [0x1]

(...)\Compatibility Assistant\Persisted>
```

Revelant information

```
--------------------------------------------------------------------------------
--------------------------------
```

UserAssist is a method used to populate a user’s start menu with
frequently used applications. This is achieved by maintaining a count
of application use in each users NTUSER.DAT registry file.
This key is suppose to contain information about programs and
shortcuts accessed by the Windows GUI, including execution count and
the date of last execution

```
--------------------------------------------------------------------------------
--------------------------------


HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
{user-ID}\Count
********************************************************************************
*****************

[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Users/info
rmant/NTUSER.DAT -p userassist
Launching userassist2 v.20130603
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Sun Mar 22 14:35:01 2015 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Wed Mar 25 15:28:47 2015 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (1)
Wed Mar 25 15:24:48 2015 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\WINWORD.EXE (
4)
Wed Mar 25 15:21:30 2015 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Google\Drive\googledrivesync.exe (1)
Wed Mar 25 15:15:50 2015 Z
```

```
  {6D809377-6AF0-444B-8957-A3773F02200E}\CCleaner\CCleaner64.exe (1)
Wed Mar 25 15:12:28 2015 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Eraser\Eraser.exe (1)
Wed Mar 25 14:57:56 2015 Z
  C:\Users\informant\Desktop\Download\ccsetup504.exe (1)
Wed Mar 25 14:50:14 2015 Z
  C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe (1)
Wed Mar 25 14:46:05 2015 Z
  Microsoft.InternetExplorer.Default (5)
Wed Mar 25 14:42:47 2015 Z
  Microsoft.Windows.MediaPlayer32 (1)
Wed Mar 25 14:41:03 2015 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\OUTLOOK.EXE (
5)
Tue Mar 24 21:05:38 2015 Z
  Chrome (7)
Tue Mar 24 18:31:55 2015 Z
  Microsoft.Windows.StickyNotes (13)
Tue Mar 24 14:16:37 2015 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe (1)
Mon Mar 23 20:27:33 2015 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\POWERPNT.EXE
(2)
Mon Mar 23 20:26:50 2015 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\EXCEL.EXE (1)
Mon Mar 23 20:10:19 2015 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (4)
Sun Mar 22 15:24:47 2015 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\slui.exe (3)
Sun Mar 22 15:12:32 2015 Z
  C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe (1)
Sun Mar 22 14:33:13 2015 Z
  Microsoft.Windows.GettingStarted (14)
  Microsoft.Windows.MediaCenter (13)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (12)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (9)
  Microsoft.Windows.RemoteDesktop (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe (7)
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Games\Solitaire\solitaire.exe
 (6)

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Wed Mar 25 15:21:30 2015 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Google Drive\Google Drive.lnk (1)
Wed Mar 25 15:15:50 2015 Z
  C:\Users\Public\Desktop\CCleaner.lnk (1)
Wed Mar 25 15:12:28 2015 Z
  C:\Users\Public\Desktop\Eraser.lnk (1)
Wed Mar 25 14:46:05 2015 Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer.lnk (5)
Wed Mar 25 14:42:47 2015 Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Media Player.lnk (1)
Wed Mar 25 14:41:03 2015 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Outlook 2013.lnk
(5)
Tue Mar 24 21:05:38 2015 Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Google Chrome.lnk (5)
Tue Mar 24 18:32:15 2015 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Word 2013.lnk (1)
```

```
Tue Mar 24 18:31:55 2015 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (13)
Tue Mar 24 18:29:07 2015 Z
  ::{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}\{00D8862B-6453-4957-A821-3D98D74C76BE
} (7)
Mon Mar 23 17:26:50 2015 Z
  C:\Users\Public\Desktop\Google Chrome.lnk (2)
Sun Mar 22 14:33:13 2015 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk (14)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Media Center.lnk (13)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (12)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (10)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (9)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.l
nk (8)
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk (
7)
```

```
================================================================================
======
Comments
================================================================================
======
```

http://www.reydes.com/d/?q=Forense_a_UserAssist_en_Windows

```
[leviathan3773@latitude:~ ] $ echo "{6Q809377-6NS0-444O-8957-N3773S02200R}\Renfr
e\Renfre.rkr" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
{6D809377-6AF0-444B-8957-A3773F02200E}\Eraser\Eraser.exe
```

Useful information to Bash/Python scripts
----
https://www.aldeid.com/wiki/Windows-userassist-keys

15 . List all traces about the system on/off and the user logon/logoff.
(It should be considered only during a time range between 09:00 and 18:00 in the timezone from Question 4.)

```
[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Windows/Sy
stem32/config/SOFTWARE -p winlogon
Launching winlogon v.20130425
winlogon v.20130425
(Software) Get values from the WinLogon key

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Wed Mar 25 13:05:43 2015 (UTC)
  LegalNoticeCaption = 
  LegalNoticeText = 
  ReportBootOk = 1
  AutoRestartShell = 1
  ForceUnlockLogon = 0
  PasswordExpiryWarning = 5
  PowerdownAfterShutdown = 0
  ShutdownWithoutLogon = 0
  WinStationsDisabled = 0
  DisableCAD = 1
  scremoveoption = 0
  AutoAdminLogon = 0
  CachedLogonsCount = 10
  DebugServerCommand = no
  ShutdownFlags = 43
  Background = 0 0 0
  DefaultUserName = informant
  Shell = explorer.exe
  Userinit = C:\Windows\system32\userinit.exe,
  PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
  VMApplet = SystemPropertiesPerformance.exe /pagefile

Notify subkey not found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
  DefaultDomainName =
  DefaultUserName =
  ReportBootOk = 1
  Shell = explorer.exe
  Userinit = userinit.exe
  PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
  VMApplet = SystemPropertiesPerformance.exe /pagefile

Notify subkey not found.
```

17 . What web browsers were used?

Internet explorer and Google chrome.

```
Google chrome HKU\informant\Software\Google\Chrome\BLBeacon (value: version)
-----------------------------------------------------------------------------
HKU\Software\Google\Chrome\BLBeacon> cat version
Value <version> of type REG_SZ (1), data length 28 [0x1c]
41.0.2272.101


HKU\Software\Google\Chrome\BLBeacon> cat state
Value <state> of type REG_DWORD (4), data length 4 [0x4]
0x00000001

HKU\Software\Google\Chrome\BLBeacon> cat failed_count
Value <failed_count> of type REG_DWORD (4), data length 4 [0x4]
0x00000000


Internet explorer HKLM\SOFTWARE\Microsoft\Internet Explorer (value: svcVersion)
--------------------------------------------------------------------------------

\Microsoft\Internet Explorer> cat Version
Value <Version> of type REG_SZ (1), data length 32 [0x20]
9.11.9600.17691

\Microsoft\Internet Explorer> cat svcUpdateVersion
Value <svcUpdateVersion> of type REG_SZ (1), data length 16 [0x10]
11.0.17
```

18 . Identify directory/file paths related to the web browser history.

MS IE (9 or lower)

```
[leviathan3773@latitude:History ] $ pwd

FILE [/mnt/windows/hdd/Users/informant/AppData/Local/Microsoft/Windows/History]


[leviathan3773@latitude:Temporary Internet Files ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Microsoft/Windows/Temporary Internet Files

[leviathan3773@latitude:Cookies ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Roaming/Microsoft/Windows/Cookies
```

MS IE 11

```
[leviathan3773@latitude:WebCache ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Microsoft/Windows/WebCache
```

Chrome

```
[leviathan3773@latitude:Default ] $ ls -la | grep History
-rwxrwxrwx 1 root root   135168 mar 24  2015 History
-rwxrwxrwx 2 root root    16384 mar 24  2015 History-journal
-rwxrwxrwx 2 root root    47175 mar 24  2015 History Provider Cache
[leviathan3773@latitude:Default ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default

[leviathan3773@latitude:Media Cache ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default/Media Cache

[leviathan3773@latitude:GPUCache ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default/GPUCache

[leviathan3773@latitude:Default ] $ file Cookies
Cookies: SQLite 3.x database
[leviathan3773@latitude:Default ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default

[leviathan3773@latitude:Default ] $ file Extension\ Cookies
Extension Cookies: SQLite 3.x database
[leviathan3773@latitude:Default ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default

[leviathan3773@latitude:Default ] $ file Cookies
Cookies: SQLite 3.x database
[leviathan3773@latitude:Default ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default
```

19 . What websites were the suspect accessing? (Timestamp, URL...)

Accesing databases files...

```
DDBB [/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Default]
```

```
[leviathan3773@latitude:Default ] $ file * | grep SQLite
Cookies:                          SQLite 3.x database - REVISADA ** Useful infor
mation
Extension Cookies:                SQLite 3.x database - REVISADA
Favicons:                         SQLite 3.x database - REVISADA
History:                          SQLite 3.x database - REVISADA ** Useful infor
mation
Login Data:                       SQLite 3.x database - REVISADA
Network Action Predictor:         SQLite 3.x database - REVISADA
Origin Bound Certs:               SQLite 3.x database - REVISADA
QuotaManager:                     SQLite 3.x database - REVISADA
Shortcuts:                        SQLite 3.x database - REVISADA
Top Sites:                        SQLite 3.x database - REVISADA
Web Data:                         SQLite 3.x database - REVISADA


File [/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Def
ault/History]
sqlite> .tables
downloads             meta                  urls
downloads_url_chains  segment_usage         visit_source
keyword_search_terms  segments              visits

sqlite> select * from keyword_search_terms
   ...> ;
2|21|outlook 2013 settings|outlook 2013 settings
2|23|emmy noether|Emmy Noether
2|24|data leakage methods|data leakage methods
2|28|leaking confidential information|leaking confidential information
2|29|leaking confidential information|leaking confidential information
2|30|leaking confidential information|leaking confidential information
2|31|information leakage cases|information leakage cases
2|32|information leakage cases|information leakage cases
2|35|information leakage cases|information leakage cases
2|36|information leakage cases|information leakage cases
2|37|information leakage cases|information leakage cases
2|38|information leakage cases|information leakage cases
2|41|intellectual property theft|intellectual property theft
2|46|how to leak a secret|how to leak a secret
2|49|cloud storage|cloud storage
2|54|digital forensics|digital forensics
2|61|how to delete data|how to delete data
2|62|anti-forensics|anti-forensics
2|67|system cleaner|system cleaner
2|68|system cleaner|system cleaner
2|69|how to recover data|how to recover data
2|70|how to recover data|how to recover data
2|71|how to recover data|how to recover data
2|72|data recovery tools|data recovery tools
2|77|google|google
2|78|apple icloud|apple icloud
2|90|google drive|google drive
2|116|security checkpoint cd-r|security checkpoint cd-r


--------------------------------------------------------------------------------
-------------------------------------
```

```
sqlite> select * from segments;
1|https://google.com/|19
2|http://bing.com/|20

["[Google Chrome's] timestamp is formatted as the number of microseconds since J
anuary, 1601"]

sqlite> SELECT url, datetime(last_visit_time / 1000000 + (strftime('%s', '1601-0
1-01')),'unixepoch') FROM urls;

http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages|2
015-03-22 15:10:24
https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clic
konceinstalled=1|2015-03-22 15:11:16
https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=in
ternet+explorer+11&gs_l=heirloom-hp.3..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1
110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w|2015-03-22
 15:10:52
http://www.msn.com/?ocid=iehp|2015-03-22 15:09:24
http://windows.microsoft.com/en-us/internet-explorer/download-ie|2015-03-22 15:1
0:50
http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explor
er/ie-11-worldwide-languages&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDAC
g&ved=0CCoQFjAB&usg=AFQjCNE7UKIWEBiWO2N96IFeo6ZywhRLfw|2015-03-22 15:09:56
http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/welcome|2015-
03-22 15:09:20
http://go.microsoft.com/fwlink/?LinkID=121792|2015-03-22 15:09:20
http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome|2015-03-22 15:
09:22
http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EA
A/IE11-Windows6.1-x64-en-us.exe|2015-03-22 15:11:06
https://www.google.com/?gws_rd=ssl|2015-03-22 15:09:40
http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explor
er/download-ie&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDACg&ved=0CB8QFjA
A&usg=AFQjCNEwsIz17kY-jTXbaWPcQDfBbVEi7A|2015-03-22 15:09:52
https://www.google.com/webhp?hl=en|2015-03-24 21:07:19
https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D
%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B68685C6D-795B-6A37-5D90-2A
B8DC4D402B%7D%26lang%3Den%26browser%3D2%26usagestats%3D0%26appname%3DGoogle%2520
Chrome%26needsadmin%3Dprefers%26brand%3DCHNG|2015-03-22 15:11:08
https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_
medium=hpp&utm_campaign=en|2015-03-22 15:11:14
http://go.microsoft.com/fwlink/?LinkId=69157|2015-03-22 15:09:02
http://tools.google.com/chrome/intl/en/welcome.html|2015-03-22 15:11:58
https://www.google.com/intl/en/chrome/browser/welcome.html|2015-03-22 15:11:58
https://www.google.com/|2015-03-24 21:05:40
http://www.bing.com/|2015-03-24 21:05:40
https://www.google.com/#q=outlook+2013+settings|2015-03-22 15:28:16
https://support.office.com/en-nz/article/Set-up-email-in-Outlook-2010-or-Outlook
-2013-for-Office-365-or-Exchange-based-accounts-6e27792a-9267-4aa4-8bb6-c84ef146
101b|2015-03-22 15:28:13
https://www.google.com/webhp?hl=en#q=Emmy+Noether&oi=ddle&ct=emmy-noethers-133rd
-birthday-5681045017985024-hp&hl=en|2015-03-23 17:27:56
https://www.google.com/webhp?hl=en#hl=en&q=data+leakage+methods|2015-03-23 18:02
:09
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&ur
l=http%3A%2F%2Fwww.sans.org%2Freading-room%2Fwhitepapers%2Fawareness%2Fdata-leak
age-threats-mitigation_1931&ei=IFUQVezLK5PnsATO3IDoBw&usg=AFQjCNGnnDJlx5Rnz6z5bV
XCIJgaCwXuaQ&bvm=bv.88528373,d.aWw&cad=rja|2015-03-23 18:02:17
http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-miti
```

```
gation_1931|2015-03-23 18:02:18
http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-miti
gation-1931|2015-03-23 18:02:18
https://www.google.com/webhp?hl=en#hl=en&q=leaking+confidential+information|2015
-03-23 18:02:44
https://www.google.com/webhp?hl=en#q=leaking+confidential+information&hl=en&star
t=10|2015-03-23 18:03:17
https://www.google.com/webhp?hl=en#q=leaking+confidential+information&hl=en&star
t=20|2015-03-23 18:03:31
https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases|2015-03-23
18:03:40
https://www.google.com/webhp?hl=en#q=information+leakage+cases&hl=en&tbm=nws|201
5-03-23 18:04:33
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=newssearch&cd=4&ved=0CCYQ
qQIoADAD&url=http%3A%2F%2Fwww.emirates247.com%2Fbusiness%2Ftechnology%2Ftop-5-so
urces-leaking-personal-data-2015-03-13-1.584027&ei=sFUQVdKvPPWZsQSC-oLgDA&usg=AF
QjCNGhQdoP0v9rKLkw4B9tET-YRTFEtw&bvm=bv.88528373,d.aWw&cad=rja|2015-03-23 18:04:
53
http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-da
ta-2015-03-13-1.584027|2015-03-23 18:04:54
https://www.google.com/webhp?hl=en#q=information+leakage+cases&hl=en|2015-03-23
18:05:15
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&source=lnms&tbm=isch&sa=X&ei=21UQVb20Eu-HsQTJ5IDAAQ&ved=0CAgQ_AUoAw|2
015-03-23 18:05:18
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1|2015-03-23 18:05:19
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#q=information+leakage+cases&hl=en|2015-03-23 18:05:22
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&ur
l=http%3A%2F%2Fwww.mediapost.com%2Fpublications%2Farticle%2F205047%2Fgoogle-to-s
ettle-data-leakage-case-for-85-mill.html%3Fedition%3D&ei=4VUQVdO8JurfsAT9ioLIBQ&
usg=AFQjCNFc5f-cGTRfFN2WeWpfm9Eli0siBg&bvm=bv.88528373,d.cWc&cad=rja|2015-03-23
18:05:27
http://www.mediapost.com/publications/article/205047/google-to-settle-data-leaka
ge-case-for-85-mill.html?edition=|2015-03-23 18:05:28
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=intellectual+property+theft|2015-03-23 18:05:48
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CB4QF
jAA&url=http%3A%2F%2Fwww.fbi.gov%2Fabout-us%2Finvestigate%2Fwhite_collar%2Fipr%2
Fipr&ei=-VUQVaXJM7iSsQT584DADw&usg=AFQjCNF7eFFsWGyvWw2jaWkVtlf-0Btddg&bvm=bv.885
28373,d.cWc&cad=rja|2015-03-23 18:05:54
http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr|2015-03-23 18:05:55
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CDEQF
jAC&url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FIntellectual_property&ei=-VUQVaXJ
M7iSsQT584DADw&usg=AFQjCNGhHfTZFaK6wQe0WVP95Go0kFfGLA&bvm=bv.88528373,d.cWc&cad=
rja|2015-03-23 18:06:01
http://en.wikipedia.org/wiki/Intellectual_property|2015-03-23 18:06:01
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=how+to+leak+a+secret|2015-03-23 18:06:27
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CCcQF
jAB&url=http%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fum%2Fpeople%2Fyael%2Fpubli
cations%2F2001-leak_secret.pdf&ei=IlYQVbbzB6uxsASbj4GgCA&usg=AFQjCNGpzaLYBk7grHE
pVoQi0fIXATFEWA&bvm=bv.88528373,d.cWc&cad=rja|2015-03-23 18:06:53
http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret
.pdf|2015-03-23 18:06:53
```

```
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=cloud+storage|2015-03-23 18:14:50
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CEUQF
jAB&url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FCloud_storage&ei=GFgQVfWtL8mPsQTr
94DADg&usg=AFQjCNH2X7RGXgS6UOnd4gSg8NmtZ6JDtQ&bvm=bv.88528373,d.cWc&cad=rja|2015
-03-23 18:15:09
http://en.wikipedia.org/wiki/Cloud_storage|2015-03-23 18:15:09
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CEwQF
jAC&url=http%3A%2F%2Fwww.pcadvisor.co.uk%2Ftest-centre%2Finternet%2F3506734%2Fbe
st-cloud-storage-dropbox-google-drive-onedrive-icloud%2F&ei=GFgQVfWtL8mPsQTr94DA
Dg&usg=AFQjCNFK5bX07QI1lKKNzlkXBEbv8LzMsg&bvm=bv.88528373,d.cWc&cad=rja|2015-03-
23 18:15:31
http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage-dropb
ox-google-drive-onedrive-icloud/|2015-03-23 18:15:32
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=digital+forensics|2015-03-23 18:15:44
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CFEQFjAF&ur
l=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FDigital_forensics&ei=UFgQVayPBOG1sQS7y4
Ew&usg=AFQjCNFU-HDPY2v07qAo1hunNjD4uG8U9Q&bvm=bv.88528373,d.cWc&cad=rja|2015-03-
23 18:15:49
http://en.wikipedia.org/wiki/Digital_forensics|2015-03-23 18:15:49
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CF0QFjAG&ur
l=http%3A%2F%2Fnij.gov%2Ftopics%2Fforensics%2Fevidence%2Fdigital%2Fpages%2Fwelco
me.aspx&ei=UFgQVayPBOG1sQS7y4Ew&usg=AFQjCNF4PYQlnERZIKDzb1fMP-T5aZLTrg&bvm=bv.88
528373,d.cWc&cad=rja|2015-03-23 18:16:05
http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx|2015-03-23 1
8:16:37
http://nij.gov/Pages/PageNotFoundError.aspx?requestUrl=http://nij.gov/topics/for
ensics/evidence/digital/standards/pages/welcome.aspx|2015-03-23 18:16:34
http://nij.gov/topics/forensics/evidence/digital/analysis/pages/welcome.aspx|201
5-03-23 18:16:42
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=how+to+delete+data|2015-03-23 18:16:55
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=anti-forensics|2015-03-23 18:17:14
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&ur
l=http%3A%2F%2Fforensicswiki.org%2Fwiki%2FAnti-forensic_techniques&ei=qlgQVa2iCs
3jsASKxICQCQ&usg=AFQjCNFPXy9OjJutWkkJNc2rdmEsnH8gmw&bvm=bv.88528373,d.cWc&cad=rj
a|2015-03-23 18:17:19
http://forensicswiki.org/wiki/Anti-forensic_techniques|2015-03-23 18:17:19
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CEcQFjAE&ur
l=https%3A%2F%2Fdefcon.org%2Fimages%2Fdefcon-20%2Fdc-20-presentations%2FPerklin%
2FDEFCON-20-Perklin-AntiForensics.pdf&ei=qlgQVa2iCs3jsASKxICQCQ&usg=AFQjCNGuYkqf
Q-eoxWMrlLOnA1MEBetVMA&bvm=bv.88528373,d.cWc&cad=rja|2015-03-23 18:17:57
https://defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON-20-Perkli
n-AntiForensics.pdf|2015-03-23 18:18:00
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=system+cleaner|2015-03-23 18:18:10
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#q=system+cleaner&hl=en&start=10|2015-03-23 18:18:15
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=how+to+recover+data|2015-03-23 18:18:30
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
```

```
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#q=how+to+recover+data&hl=en&start=20|2015-03-23 18:18:43
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#q=how+to+recover+data&hl=en&start=10|2015-03-23 18:18:46
https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&
site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dp
r=1#hl=en&q=data+recovery+tools|2015-03-23 19:47:43
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CGwQFjAG&ur
l=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FList_of_data_recovery_software&ei=F1kQV
d3EGfOHsQSAz4CIDA&usg=AFQjCNEPVfDD6BgIwmVUOVFG3RsE-3XGQA&bvm=bv.88528373,d.cWc&c
ad=rja|2015-03-23 18:19:17
http://en.wikipedia.org/wiki/List_of_data_recovery_software|2015-03-23 18:19:17
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0CIABEBYwCQ
&url=http%3A%2F%2Fwww.forensicswiki.org%2Fwiki%2FTools%3AData_Recovery&ei=F1kQVd
3EGfOHsQSAz4CIDA&usg=AFQjCNH6vSduODlbRgqX5d02tLe3fhy-sw&bvm=bv.88528373,d.cWc&ca
d=rja|2015-03-23 18:19:21
http://www.forensicswiki.org/wiki/Tools:Data_Recovery|2015-03-23 18:19:21
https://www.google.com/webhp?hl=en#hl=en&q=google|2015-03-23 19:48:19
https://www.google.com/webhp?hl=en#hl=en&q=apple+icloud|2015-03-23 19:55:09
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCUQFjAB&ur
l=https%3A%2F%2Fwww.apple.com%2Ficloud%2F&ei=nm8QVc_BC8vasATi_IGoBA&usg=AFQjCNEG
tiW1BO4CUv7JdC2GJrvivhQAZg&bvm=bv.88528373,d.aWw&cad=rja|2015-03-23 19:55:17
https://www.apple.com/icloud/|2015-03-23 19:55:18
https://www.apple.com/icloud/setup/pc.html|2015-03-23 19:55:28
http://www.icloud.com/icloudcontrolpanel|2015-03-23 19:55:34
https://www.icloud.com/icloudcontrolpanel|2015-03-23 19:55:34
http://www.icloud.com/icloudcontrolpanel/|2015-03-23 19:55:34
https://www.icloud.com/icloudcontrolpanel/|2015-03-23 19:55:34
http://support.apple.com/kb/DL1455|2015-03-23 19:55:35
https://support.apple.com/kb/DL1455|2015-03-23 19:55:35
http://support.apple.com/kb/DL1455?locale=en_US|2015-03-23 19:55:35
https://support.apple.com/kb/DL1455?locale=en_US|2015-03-23 19:55:35
https://www.google.com/webhp?hl=en#hl=en&q=google+drive|2015-03-23 19:56:04
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&ur
l=https%3A%2F%2Fwww.google.com%2Fdrive%2F&ei=1G8QVYfAGJK_sQSE-oCAAQ&usg=AFQjCNEk
d59bGLZR6pLjNvtXxR3vGLBE9Q&bvm=bv.88528373,d.aWw&cad=rja|2015-03-23 19:56:08
https://www.google.com/drive/|2015-03-23 19:56:08
https://www.google.com/drive/download/|2015-03-23 19:56:15
https://tools.google.com/dlpage/drive/index.html?hl=en#eula|2015-03-23 19:56:19
https://tools.google.com/dlpage/drive/thankyou.html?hl=en|2015-03-23 19:56:28
https://news.google.com/nwshp?hl=en&tab=wn&ei=xnARVdWfPPLjsASdgIKoAw&ved=0CAUQqS
4oBQ|2015-03-24 15:22:04
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=0b2226a6a5
dab3b27ee85fc5e8d21f28f01e|2015-03-24 15:22:46
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04|2015-03-24 15:23:16
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427212899|2015-03-24 16:01:39
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427213801|2015-03-24 16:16:41
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427214703|2015-03-24 16:31:43
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427215604|2015-03-24 16:46:44
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427216506|2015-03-24 17:01:45
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427217407|2015-03-24 17:16:47
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
```

```
5cb189b8dd7fd58ef6bc922ec04&ar=1427218623|2015-03-24 17:37:03
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427219526|2015-03-24 17:52:06
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427220429|2015-03-24 18:07:09
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427221332|2015-03-24 18:22:12
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f817
5cb189b8dd7fd58ef6bc922ec04&ar=1427222627|2015-03-24 18:43:47
https://news.google.com/news?pz=1&cf=all&ned=us&siidp=0c33ef04190b3734a22c5bae18
801ff1041e|2015-03-24 18:59:52
http://www.cbsnews.com/news/germanwings-flight-9525-pulverized-plane-parts-rough
-mountain-terrain/|2015-03-24 19:00:04
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=538c61c825
aba06be7485be747a619778015|2015-03-24 19:00:27
https://news.google.com/news?pz=1&cf=all&ned=us&siidp=f206159a77e2be8861b5231ddc
055443b303|2015-03-24 19:00:53
https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=s&siidp=545d9217fe
5452fcfbcbe251400793f398ac|2015-03-24 19:00:57
https://news.google.com/news?pz=1&hl=en&tab=nn|2015-03-24 19:01:18
https://www.google.com/#q=security+checkpoint+cd-r|2015-03-24 21:06:50

--------------------------------------------------------------------------------
-------------------------------------

File [/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Def
ault/Cookies]

sqlite> select * from cookies;
13071510721576390|.youtube.com|VISITOR_INFO1_LIVE||/|13092548701576390|0|1|13071
697258519381|1|1|1|
13071510721576506|.youtube.com|YSC||/|0|0|1|13071697258519381|0|0|1|
13071510726538603|.google.com|__utma||/intl/en/chrome/browser/|13134582726000000
|0|0|13071510726538603|1|1|1|
13071510726538906|.google.com|__utmc||/intl/en/chrome/browser/|0|0|0|13071510726
538906|0|0|1|
13071510726539047|.google.com|__utmz||/intl/en/chrome/browser/|13087278726000000
|0|0|13071510726539047|1|1|1|
13071510727057405|.google.com|PREF||/|13134582727057405|0|0|13071704800185894|1|
1|1|
13071510730843693|.bing.com|_FS||/|0|0|0|13071704840917015|0|0|1|
13071510730843943|www.bing.com|SRCHUID||/|13134582731843943|0|0|1307170484091701
5|1|1|1|
13071510730844041|.bing.com|SRCHUSR||/|13134582731844041|0|0|13071704840917015|1
|1|1|
13071510730844115|.bing.com|_EDGE_S||/|0|0|1|13071704840917015|0|0|1|
13071510730844204|.bing.com|_EDGE_V||/|13134582731844204|0|1|13071704840917015|1
|1|1|
13071510730844370|www.bing.com|MUIDB||/|13134582731844370|0|1|13071704840917015|
1|1|1|
13071510731335826|.bing.com|_RwBf||/|13134582731000000|0|0|13071704840917015|1|1
|1|
13071510731628253|ssl.bing.com|SRCHUID||/|13134582732628253|0|0|1307170474396818
7|1|1|1|
13071510732367181|ssl.bing.com|MUIDB||/|13134582732367181|0|1|13071704743968187|
1|1|1|
13071510734087683|a4.bing.com|SRCHUID||/|13134582734087683|0|0|13071704745750591
|1|1|1|
13071511656703442|.bing.com|SRCHD||/|13134583656703442|0|0|13071704840917015|1|1
|1|
13071511694668641|.office.com|detmkt||/|0|1|1|13071511694668641|0|0|1|
13071511695338722|.office.com|MSFPC||/|13134583695000000|0|0|13071511695338722|1
|1|1|
13071511695434044|ots.optimize.webtrends.com|JSESSIONID||/ots|0|0|0|130715116954
34044|0|0|1|
13071511695494449|support.office.com|c.ms.ocpub.assetID||/en-nz/article|0|0|0|13
071511695494449|0|0|1|
13071511695522603|.bing.com|MUID||/|13134583695522603|0|0|13071704840917015|1|1|
1|
13071511695522720|.c.bing.com|MR||/|13087063695522720|0|0|13071511695522720|1|1|
1|
13071511695522800|.c.bing.com|SRM_B||/|13134583695522800|0|0|13071511695522800|1
|1|1|
13071511695522879|.c.bing.com|SRM_I||/|13134583695522879|0|0|13071511695522879|1
|1|1|
13071511695550375|support.office.com|MC0||/en-nz/article|0|0|0|13071511695550375
|0|0|1|
13071511695683335|.c1.microsoft.com|SM||/|0|0|0|13071511695683335|0|0|1|
13071511695683427|.microsoft.com|MUID||/|13134583695683427|0|0|13071607613457902
|1|1|1|
13071511695683523|.c1.microsoft.com|MR||/|13087063695683523|0|0|1307151169568352
3|1|1|1|
13071511695871866|.microsoft.com|MC1||/|13134583695871866|0|0|13071607613457902|
1|1|1|
13071511695872069|.microsoft.com|A||/|13134583695872069|0|0|13071607613457902|1|
1|1|
13071605278324624|.google.com|SNID||/verify|13087416478324624|0|1|13071607397657
444|1|1|1|
13071607397797800|.google.com|NID||/|13087418597797800|0|1|13071704800185894|1|1
|1|
13071607498270692|.emirates247.com|__utma||/|13134679498000000|0|0|1307160749827
0692|1|1|1|
13071607498270956|.emirates247.com|__utmc||/|0|0|0|13071607498270956|0|0|1|
13071607498271022|.emirates247.com|__utmz||/|13087375498000000|0|0|1307160749827
1022|1|1|1|
13071607498337161|.emirates247.com|__gads||/|13134679497000000|0|0|1307160749833
7161|1|1|1|
13071607501786270|www.emirates247.com|tmpPersistentuserId||/|13103143501786270|0
|0|13071607501786270|1|1|1|
13071607502225285|.hit.gemius.pl|Gtest||/|13236998401225285|0|0|1307160750222528
5|1|1|1|
13071607502633558|.hit.gemius.pl|Gdyn||/|13236998401633558|0|0|13071607502633558
|1|1|1|
13071607502961704|.effectivemeasure.net|t||/|13103143502000000|0|0|1307160750296
1704|1|1|1|
13071607503386555|.effectivemeasure.net|vt||/|13102711503386555|0|0|130716075033
86555|1|1|1|
13071607503395411|.emirates247.com|_em_vt||/|13102711503000000|0|0|1307160750339
5411|1|1|1|
13071607503417463|.twitter.com|pid||/|13118868303417463|0|0|13071697213503221|1|
1|1|
13071607506198932|.disqus.com|disqus_unique||/|13103143506000000|0|0|13071608135
309690|1|1|1|
13071607507054388|.disqus.com|__utma||/|13134679507000000|0|0|13071608135309690|
1|1|1|
13071607507054887|.disqus.com|__utmc||/|0|0|0|13071608135309690|0|0|1|
13071607507055089|.disqus.com|__utmz||/|13087375507000000|0|0|13071608135309690|
1|1|1|
13071607507241865|.quantserve.com|mc||/|13118954707241865|0|0|13071608138579885|
1|1|1|
13071607507294478|.mookie1.com|id||/|13074199507294478|0|0|13071607507294478|1|1
|1|
13071607507294578|.mookie1.com|mdata||/|13074199507294578|0|0|13071607507294578|
1|1|1|
13071607507697760|.crwdcntrl.net|_cc_aud||/|13094935507697760|0|0|13071607507697
760|1|1|1|
13071607507697870|.crwdcntrl.net|_cc_cc||/|13094935507697870|0|0|130716075076978
70|1|1|1|
13071607507698163|.crwdcntrl.net|_cc_id||/|13094935507698163|0|0|130716075076981
63|1|1|1|
13071607507698252|.crwdcntrl.net|_cc_dc||/|13072471507698252|0|0|130716075076982
52|1|1|1|
13071607508607456|www.linkedin.com|L1e||/|0|0|0|13071697216401785|0|0|1|
13071607508607534|.linkedin.com|bcookie||/|13134721360607534|0|0|130716972137879
92|1|1|1|
13071607508607599|.www.linkedin.com|bscookie||/|13134721360607599|1|1|1307169721
6401785|1|1|1|
13071607528916188|www.mediapost.com|csrftoken||/|13103057128916188|0|0|130716075
28916188|1|1|1|
13071607530142868|.doubleclick.net|id||/|13134679530142868|0|0|13071697208911217
|1|1|1|
13071607530374614|.mediapost.com|_ga||/|13134679530000000|0|0|13071607530374614|
1|1|1|
13071607530955311|.mediapost.com|__gads||/|13134679529000000|0|0|130716075309553
11|1|1|1|
13071607533075760|bam.nr-data.net|JSESSIONID||/|0|0|0|13071607533075760|0|0|1|
13071607556977088|.fbi.gov|fsr.paused||/|0|0|0|13071607556977088|0|0|1|
13071607557913756|.fbi.gov|__utma||/|13134679557000000|0|0|13071607557913756|1|1
|1|
13071607557914291|.fbi.gov|__utmc||/|0|0|0|13071607557914291|0|0|1|
13071607557914412|.fbi.gov|__utmz||/|13087375557000000|0|0|13071607557914412|1|1
|1|
13071607560531259|.dsply.com|adc||/|0|0|0|13071607560531259|0|0|1|
13071607560531348|www.dsply.com|PHPSESSID||/|0|0|0|13071607560531348|0|0|1|
13071607560531385|.dsply.com|ub_uuid||/|13387226760531385|0|0|13071607560531385|
1|1|1|
13071607560531487|.dsply.com|nitpo||/|13387226760531487|0|0|13071607560531487|1|
1|1|
13071607561429691|.wikipedia.org|GeoIP||/|0|0|0|13071608357620584|0|0|1|
13071607564247377|.wikimedia.org|GeoIP||/|0|0|0|13071608357910597|0|0|1|
13071607564820544|en.wikipedia.org|uls-previous-languages||/|0|0|0|1307160835762
0584|0|0|1|
13071607565801857|en.wikipedia.org|mediaWiki.user.sessionId||/|0|0|0|13071608357
620584|0|0|1|
13071607578554495|gateway.answerscloud.com|fsr.STORAGE||/fbi-gov/production/fore
see|0|0|0|13071607578554495|0|0|1|
13071607579302769|gateway.answerscloud.com|_IFR_fbi.gov_fsr.a||/|0|0|0|130716075
79302769|0|0|1|
13071607579552851|.fbi.gov|fsr.a||/|0|0|0|13071607579552851|0|0|1|
13071607579658795|.fbi.gov|fsr.s||/|0|0|0|13071607579658795|0|0|1|
13071608132132667|.pcadvisor.co.uk|__cfduid||/|13103144132132667|0|1|13071608132
132667|1|1|1|
13071608134896698|.bluekai.com|bklc||/|13087160134896698|0|0|13071608134896698|1
|1|1|
13071608134896742|.bluekai.com|bko||/|13087160134896742|0|0|13071608134896742|1|
1|1|
13071608134896832|.bluekai.com|bkw5||/|13087160134896832|0|0|13071608134896832|1
|1|1|
13071608134968502|engine.instinctiveads.com|__inst_v||/|13103230535968502|0|0|13
071608134968502|1|1|1|
13071608135000279|www.pcadvisor.co.uk|__inst_v||/|26504677439900000|0|0|1307160
8135000279|1|1|1|
13071608135010721|.visiblemeasures.com|uid||/|13103144135010721|0|0|130716081350
10721|1|1|1|
13071608135010812|.visiblemeasures.com|sid||/|0|0|0|13071608135010812|0|0|1|
13071608135015365|.criteo.com|uid||/|13103144134015365|0|0|13071608135015365|1|1
|1|
13071608135015447|.criteo.com|udc||/|13087505735015447|0|0|13071608135015447|1|1
|1|
13071608135015495|.criteo.com|zdi||/|13087505735015495|0|0|13071608135015495|1|1
|1|
13071608135129671|.bluekai.com|bkc||/|13087160135129671|0|0|13071608135129671|1|
1|1|
13071608135129899|.bluekai.com|bkdc||/|13087160135129899|0|0|13071608135129899|1
|1|1|
13071608135130131|.bluekai.com|bkst||/|13087160135130131|0|0|13071608135130131|1
|1|1|
13071608135130277|.bluekai.com|bku||/|13087160135130277|0|0|13071608135130277|1|
1|1|
13071608135379748|.pcadvisor.co.uk|CFID||/|0|0|1|13071608135379748|0|0|1|
13071608135379921|.pcadvisor.co.uk|CFTOKEN||/|0|0|1|13071608135379921|0|0|1|
13071608135914733|.outbrain.com|obuid||/|13079384135000000|0|0|13071697206574664
|1|1|1|
13071608136057620|.jsrdn.com|u||/|13791945602057620|0|0|13071608136057620|1|1|1|
13071608136544130|.macworld.co.uk|__cfduid||/|13103144136544130|0|1|130716081365
44130|1|1|1|
13071608136737915|.unrulymedia.com|unruly_u||/|13134680136737915|0|0|13071608136
737915|1|1|1|
13071608136738128|.unrulymedia.com|uid||/|13134680136738128|0|0|1307160813673812
8|1|1|1|
13071608136880166|.pcadvisor.co.uk|_ga||/|13134680136000000|0|0|1307160813688016
6|1|1|1|
13071608137277540|.pcadvisor.co.uk|__gads||/|13134680135000000|0|0|1307160813727
7540|1|1|1|
13071608137517442|.outbrain.com|_lvs2||/|13105476936000000|0|0|13071697206574664
|1|1|1|
13071608137517688|.outbrain.com|_lvd2||/|13072172616000000|0|0|13071697206574664
|1|1|1|
13071608137517927|.outbrain.com|_rcc2||/|13105476936000000|0|0|13071697206574664
|1|1|1|
13071608137518112|.outbrain.com|_fcap_CAM4||/|13072212936000000|0|0|130716972065
74664|1|1|1|
13071608137518413|.outbrain.com|_ofcap_DOC1||/|13072212936000000|0|0|13071697206
574664|1|1|1|
13071608137518609|.outbrain.com|_utastes_1||/|13132088136000000|0|0|130716972065
74664|1|1|1|
13071608139034101|.scorecardresearch.com|UID||/|13133816139034101|0|0|1307169721
0311780|1|1|1|
13071608139035114|.scorecardresearch.com|UIDR||/|13133816139035114|0|0|130716972
10311780|1|1|1|
13071608139088246|.ayads.co|__cfduid||/|13103144139088246|0|1|13071608139088246|
1|1|1|
13071608166570595|nij.gov|SPUsageId||/|13072817767570595|0|1|13071608166570595|1
|1|1|
13071608203475571|.nij.gov|_ga||/|13134680203000000|0|0|13071608203475571|1|1|1|
13071608203934418|.nij.gov|__utma||/|13134680203000000|0|0|13071608203934418|1|1
|1|
13071608203934834|.nij.gov|__utmc||/|0|0|0|13071608203934834|0|0|1|
13071608203934954|.nij.gov|__utmz||/|13087376203000000|0|0|13071608203934954|1|1
|1|
13071608204100514|nij.gov|WSS_FullScreenMode||/|0|0|0|13071608204100514|0|0|1|
13071608204309980|.nij.gov|fsr.s||/|0|0|0|13071608204309980|0|0|1|
13071614139639691|.apple.com|s_cc||/|0|0|0|13071617018471618|0|0|1|
13071614139655762|.apple.com|s_orientation||/|0|0|0|13071617018471618|0|0|1|
13071614139664628|.apple.com|s_vnum_n2_us||/|13229294139000000|0|0|1307161701847
1618|1|1|1|
13071614139726312|.apple.com|POD||/|13074033339000000|0|0|13071617018471618|1|1|
1|
13071614141656888|.apple.com|s_orientationHeight||/|0|0|0|13071617018471618|0|0|
1|
13071614141659388|.apple.com|ac_history||/|0|0|0|13071617018471618|0|0|1|
13071614145188703|.apple.com|s_fid||/|13134772545000000|0|0|13071617018471618|1|
1|1|
13071614145213454|.apple.com|s_sq||/|0|0|0|13071617018471618|0|0|1|
13071614145978407|.apple.com|s_vi||/|13134686145978407|0|0|13071617018471618|1|1
|1|
13071614175451093|.google.com|__utma||/drive/|13134686175000000|0|0|130716141754
51093|1|1|1|
13071614175451612|.google.com|__utmc||/drive/|0|0|0|13071614175451612|0|0|1|
13071614175452088|.google.com|__utmz||/drive/|13087382175000000|0|0|130716141754
52088|1|1|1|
13071614175663282|.google.com|__utma||/a/|13134686175000000|0|0|1307161417566328
2|1|1|1|
13071614175663905|.google.com|__utmc||/a/|0|0|0|13071614175663905|0|0|1|
13071614175664197|.google.com|__utmz||/a/|13087382175000000|0|0|1307161417566419
7|1|1|1|
13071614175665766|.google.com|__utma||/apps/|13134686175000000|0|0|1307161417566
5766|1|1|1|
13071614175666305|.google.com|__utmc||/apps/|0|0|0|13071614175666305|0|0|1|
13071614175666450|.google.com|__utmz||/apps/|13087382175000000|0|0|1307161417566
6450|1|1|1|
13071614175670236|.google.com|__utma||/work/apps/business/|13134686175000000|0|0
|13071614175670236|1|1|1|
13071614175670813|.google.com|__utmc||/work/apps/business/|0|0|0|130716141756708
13|0|0|1|
13071614175671046|.google.com|__utmz||/work/apps/business/|13087382175000000|0|0
|13071614175671046|1|1|1|
13071614175672815|.google.com|__utma||/intl/|13134686175000000|0|0|1307161417567
2815|1|1|1|
13071614175674213|.google.com|__utmc||/intl/|0|0|0|13071614175674213|0|0|1|
13071614175674295|.google.com|__utmz||/intl/|13087382175000000|0|0|1307161417567
4295|1|1|1|
13071614175675349|.google.com|__utma||/intx/|13134686175000000|0|0|1307161417567
5349|1|1|1|
13071614175675798|.google.com|__utmc||/intx/|0|0|0|13071614175675798|0|0|1|
13071614175676040|.google.com|__utmz||/intx/|13087382175000000|0|0|1307161417567
6040|1|1|1|
13071614175678606|.google.com|__utma||/work/|13134686175000000|0|0|1307161417567
8606|1|1|1|
13071614175679017|.google.com|__utmc||/work/|0|0|0|13071614175679017|0|0|1|
13071614175680890|.google.com|__utmz||/work/|13087382175000000|0|0|1307161417568
0890|1|1|1|
13071614179754355|.google.com|__utma||/drive/download/|13134686179000000|0|0|130
71614179754355|1|1|1|
13071614179754915|.google.com|__utmc||/drive/download/|0|0|0|13071614179754915|0
|0|1|
13071614179755349|.google.com|__utmz||/drive/download/|13087382179000000|0|0|130
71614179755349|1|1|1|
13071614181110401|tools.google.com|iid||/dlpage/drive|0|0|0|13071614181110401|0|
0|1|
13071697204292136|.cbsnews.com|fly_device||/|13072302003292136|0|0|1307169720429
2136|1|1|1|
13071697204292509|.cbsnews.com|fly_geo||/|13072302003292509|0|0|1307169720429250
9|1|1|1|
13071697205795139|.cbsnews.com|optimizelySegments||/|13387057205000000|0|0|13071
697205795139|1|1|1|
13071697205800157|.cbsnews.com|optimizelyEndUserId||/|13387057205000000|0|0|1307
1697205800157|1|1|1|
13071697205801242|.cbsnews.com|optimizelyBuckets||/|13387057205000000|0|0|130716
97205801242|1|1|1|
13071697207497786|www.cbsnews.com|cbsnews_ad||/|0|0|0|13071697207497786|0|0|1|
13071697209008973|.cbsnews.com|first_page_today||/|13071729599000000|0|0|1307169
7209008973|1|1|1|
13071697209029169|.cbsnews.com|utag_main||/|13103233209000000|0|0|13071697209029
169|1|1|1|
13071697209473069|.cbsnews.com|__gads||/|13134769209000000|0|0|13071697209473069
|1|1|1|
13071697209616528|.cbsnews.com|CBS_INTERNAL||/news/germanwings-flight-9525-pulve
rized-plane-parts-rough-mountain-terrain|13087249209000000|0|0|13071697209616528
|1|1|1|
13071697210081158|www.cbsnews.com|LDCLGFbrowser||/|13387057210000000|0|0|1307169
7210081158|1|1|1|
13071697210285552|.cbsi.com|XCLGFbrowser||/|13387230010285552|0|0|13071697210285
552|1|1|1|
13071697210287317|.cbsnews.com|prevPageType||/|0|0|0|13071697210287317|0|0|1|
13071697210289526|.cbsnews.com|s_vnum||/|13074289210000000|0|0|13071697210289526
|1|1|1|
13071697210291918|.cbsnews.com|s_getNewRepeat||/|13074289210000000|0|0|130716972
10291918|1|1|1|
13071697210292868|.cbsnews.com|s_lv_undefined||/|13166305210000000|0|0|130716972
10292868|1|1|1|
13071697210424595|www.cbsnews.com|XCLGFbrowser||/|13387057210000000|0|0|13071697
210424595|1|1|1|
13071697210490721|www.cbsnews.com|QSI_HistorySession||/|0|0|0|13071697210490721|
0|0|1|
13071697210521053|.mxptint.net|mxpim||/|13134855610521053|0|0|13071697210521053|
1|1|1|
13071697210552549|.demdex.net|demdex||/|13134769211000000|0|0|13071697210552549|
1|1|1|
13071697210696344|.imrworldwide.com|IMRID||/|13134769210696344|0|0|1307169721069
6344|1|1|1|
13071697210865997|.revsci.net|pudm_AAAA||/|13103233210865997|0|0|130716972108659
97|1|1|1|
13071697210866135|.revsci.net|NETID01||/|13105393210866135|0|0|13071697210866135
|1|1|1|
13071697210866223|.revsci.net|rtc_AAAA||/|13103233210866223|0|0|1307169721086622
3|1|1|1|
13071697210866296|.revsci.net|rts_AAAA||/|13103233210866296|0|0|1307169721086629
6|1|1|1|
13071697210896398|.doubleclick.net|_drt_||/|13071740410896398|0|1|13071697210896
398|1|1|1|
13071697210923806|.ads.pointroll.com|PRTEST||/|13134769210923806|0|0|13071697210
923806|1|1|1|
13071697210947622|.w55c.net|wfivefivec||/|13134855611947622|0|0|1307169721094762
2|1|1|1|
13071697211054704|.cbsi.com|s_vi||/|13134769211054704|0|0|13071697211054704|1|1|
1|
13071697211054778|.cbsi.com|AMCV_10D31225525FF5790A490D4D%40AdobeOrg||/|13134696
211054778|0|0|13071697211054778|1|1|1|
13071697211078874|.254a.com|tuuid||/|13074289211078874|0|0|13071697211078874|1|1
```

```
|1|
13071697211224738|.cbsnews.com|AMCV_10D31225525FF5790A490D4D%40AdobeOrg||/|13134
855611000000|0|0|13071697211224738|1|1|1|
13071697211226838|.cbsnews.com|s_cc||/|0|0|0|13071697211226838|0|0|1|
13071697211240738|.cbsnews.com|s_sq||/|0|0|0|13071697211240738|0|0|1|
13071697211317105|.yahoo.com|B||/|13134769211317105|0|0|13071697211317105|1|1|1|
13071697211340606|s.yimg.com|ywandp||/|13387057211000000|0|0|13071697211340606|1
|1|1|
13071697211853590|.cbsnews.com|aam_uuid||/|13074289211000000|0|0|130716972118535
90|1|1|1|
13071697212581474|s.yimg.com|fpc||/|13103233212000000|0|0|13071697212581474|1|1|
1|
13071697212740119|www.cbsnews.com|fly_img||/|13103233212000000|0|0|1307169721274
0119|1|1|1|
13071697213608491|www.cbsnews.com|sq4YFvJMK2||/|13569397200000000|0|0|1307169721
3608491|1|1|1|
13071697213609067|www.cbsnews.com|hycw4hSBtd||/|13072334399000000|0|0|1307169721
3609067|1|1|1|
13071697213609330|www.cbsnews.com|JYaH5Y2vxL||/|13071729599000000|0|0|1307169721
3609330|1|1|1|
13071697213609860|www.cbsnews.com|gebDnVVAmj||/|13569397200000000|0|0|1307169721
3609860|1|1|1|
13071697213802429|www.cbsnews.com|cbsArticleAuto||/|13074289213000000|0|0|130716
97213802429|1|1|1|
13071697213811840|.twitter.com|guest_id||/|13134769213811840|0|0|130716972138118
40|1|1|1|
13071697213891316|.reddit.com|__cfduid||/|13103233213891316|0|1|1307169721389131
6|1|1|1|
13071697213953763|www.stumbleupon.com|su_bc||/|13074289213953763|0|0|13071697213
953763|1|1|1|
13071697214661889|.demdex.net|dextp||/|13590097214000000|0|0|13071697214661889|1
|1|1|
13071697214686426|.addthis.com|uid||/|13134769214686426|0|0|13071697214686426|1|
1|1|
13071697214686531|.addthis.com|um||/|13134769214686531|0|0|13071697214686531|1|1
|1|
13071697214934380|.dpm.demdex.net|dpm||/|13134769215000000|0|0|13071697214934380
|1|1|1|
13071697215009221|.exelator.com|ud||/|13082065215009221|0|0|13071697215009221|1|
1|1|
13071697215372027|.bizographics.com|BizoID||/|13087465215372027|0|0|130716972153
72027|1|1|1|
13071697215372134|.bizographics.com|BizoData||/|13087465215372134|0|0|1307169721
5372134|1|1|1|
13071697216049088|.btrll.com|BR_APS||/|13103233216049088|0|1|13071697216049088|1
|1|1|
13071697216271749|pix.btrll.com|cap_608272||/|13072302016271749|0|1|130716972162
71749|1|1|1|
13071697216672253|.acxiom-online.com|ACX_COUNT||/|13103233216672253|0|0|13071697
216672253|1|1|1|
13071697216672347|.acxiom-online.com|ACXID||/|13103233216672347|0|0|130716972166
72347|1|1|1|
13071697216804599|.demdex.net|DPM||/|13134769217000000|0|0|13071697216804599|1|1
|1|
13071697216863171|.everesttech.net|gglck||/|13074289216863171|0|0|13071697216863
171|1|1|1|
13071697216863283|.everesttech.net|ev_t||/|13074289216863283|0|0|130716972168632
83|1|1|1|
13071697216863366|.everesttech.net|everest_session_v2||/|0|0|0|13071697216863366
|0|0|1|
13071697216863424|.everesttech.net|everest_g_v2||/|13131697216863424|0|0|1307169
7216863424|1|1|1|
13071697216863501|.everesttech.net|ev_t2||/|13074289216863501|0|0|13071697216863
501|1|1|1|
13071697216893674|.adnxs.com|uuid2||/|13079473216893674|0|1|13071697216893674|1|
1|1|
13071697216893778|.adnxs.com|sess||/|13071783616893778|0|1|13071697216893778|1|1
|1|
13071697216893852|.adnxs.com|anj||/|13079473216893852|0|1|13071697216893852|1|1|
1|
13071697216948334|.rlcdn.com|ck1||/|13087249213948334|0|0|13071697216948334|1|1|
1|
13071697217003311|pixel.rubiconproject.com|c||/|0|0|0|13071697217003311|0|0|1|
13071697217083903|.linkedin.com|lidc||/|13071783617083903|0|0|13071697217083903|
1|1|1|
13071697217109427|.openx.net|i||/|13103233217109427|0|0|13071697217109427|1|1|1|
13071697217150310|.rlcdn.com|rlas3||/|13087249216150310|0|0|13071697217150310|1|
1|1|
13071697217150386|.rlcdn.com|rtn1||/|13087249213150386|0|0|13071697217150386|1|1
|1|
13071697217150444|.rlcdn.com|dids1989307702||/|13087249214150444|0|0|13071697217
150444|1|1|1|
13071697217200687|.rubiconproject.com|rpb||/|13074289217200687|0|0|1307169721720
0687|1|1|1|
13071697217200795|.rubiconproject.com|put_2181||/|13074289217200795|0|0|13071697
217200795|1|1|1|
13071697217200877|.pixel.rubiconproject.com|rpx||/|13074289217200877|0|0|1307169
7217200877|1|1|1|
13071697217200938|.rubiconproject.com|khaos||/|13087465217200938|0|0|13071697217
200938|1|1|1|
13071697217475419|.pubmatic.com|PUBMDCID||/|13079473217475419|0|0|13071697217475
419|1|1|1|
13071697281853048|.bing.com|SRCHHPGUSR||/|13134769281000000|0|0|1307170484091701
5|1|1|1|
13071704742913352|.bing.com|SCRHDN||/|0|0|0|13071704840917015|0|0|1|
13071704742927406|.bing.com|_SS||/|0|0|0|13071704840917015|0|0|1|
13071704744312989|.bing.com|FBS||/|0|0|0|13071704840917015|0|0|1|
13071704744320861|.bing.com|WLS||/|0|0|0|13071704840917015|0|0|1|
13071704744792952|login.live.com|MSPRequ||/|0|1|1|13071704744792952|0|0|1|
13071704744898496|.bing.com|_HOP||/|0|0|0|13071704840917015|0|0|1|

--------------------------------------------------------------------------------
-------------------------------------

Suspect URLs:

http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome
http://windows.microsoft.com/en-us/internet-explorer/download-ie|
http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EA
A/IE11-Windows6.1-x64-en-us.exe
http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-da
ta-2015-03-
http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr

 ...
```

20 . List all search keywords using web browsers. (Timestamp, URL, keyword...)

```
File [/mnt/windows/hdd/Users/informant/AppData/Local/Google/Chrome/User Data/Def
ault/History]
```

```
sqlite> .tables
downloads             meta                  urls
downloads_url_chains  segment_usage         visit_source
keyword_search_terms  segments              visits

sqlite> select * from keyword_search_terms
   ...> ;
2|21|outlook 2013 settings|outlook 2013 settings
2|23|emmy noether|Emmy Noether
2|24|data leakage methods|data leakage methods
2|28|leaking confidential information|leaking confidential information
2|29|leaking confidential information|leaking confidential information
2|30|leaking confidential information|leaking confidential information
2|31|information leakage cases|information leakage cases
2|32|information leakage cases|information leakage cases
2|35|information leakage cases|information leakage cases
2|36|information leakage cases|information leakage cases
2|37|information leakage cases|information leakage cases
2|38|information leakage cases|information leakage cases
2|41|intellectual property theft|intellectual property theft
2|46|how to leak a secret|how to leak a secret
2|49|cloud storage|cloud storage
2|54|digital forensics|digital forensics
2|61|how to delete data|how to delete data
2|62|anti-forensics|anti-forensics
2|67|system cleaner|system cleaner
2|68|system cleaner|system cleaner
2|69|how to recover data|how to recover data
2|70|how to recover data|how to recover data
2|71|how to recover data|how to recover data
2|72|data recovery tools|data recovery tools
2|77|google|google
2|78|apple icloud|apple icloud
2|90|google drive|google drive
2|116|security checkpoint cd-r|security checkpoint cd-r
```

21 . List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)

```
(...)\CurrentVersion\Explorer\WordWheelQuery> cat MRUListEx
Value <MRUListEx> of type REG_BINARY (3), data length 8 [0x8]
:00000  00 00 00 00 FF FF FF FF                         ........


(...)\CurrentVersion\Explorer\WordWheelQuery> cat 0
Value <0> of type REG_BINARY (3), data length 14 [0xe]
:00000  73 00 65 00 63 00 72 00 65 00 74 00 00 00       s.e.c.r.e.t...


(...)\CurrentVersion\Explorer\WordWheelQuery>
```

secret

```
[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl  -r /mnt/windows/hdd/Users/inf
ormant/NTUSER.DAT -p wordwheelquery
Launching wordwheelquery v.20100330
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key
```

```
Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Mon Mar 23 18:40:17 2015 (UTC)

Searches listed in MRUListEx order

0    secret
[leviathan3773@latitude:RegRipper2.8 ] $
```

22 . What application was used for e-mail communication?

```
Node has 2 subkeys and 2 values
  key name
  <Microsoft Outlook>
  <Windows Mail>
  size     type              value name             [value if type DWORD]
    36  1 REG_SZ             <>
   396  1 REG_SZ             <PreFirstRun>

\Clients\Mail>
```

23 . Where is the e-mail file located?

```
HKEY_USERS\Software\Microsoft\Office\15.0\Outlook\PST> ls
Node has 0 subkeys and 1 values
  size     type              value name             [value if type DWORD]
   160  1 REG_SZ             <LastCorruptStore>

HKEY_USERS\Software\Microsoft\Office\15.0\Outlook\PST> cat LastCo
Value <LastCo> of type REG_SZ (1), data length 160 [0xa0]
C:\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost

HKEY_USERS\Software\Microsoft\Office\15.0\Outlook\PST>
```

24 . What was the e-mail account used by the suspect?
iaman.informant@nist.gov

25 . List all e-mails of the suspect. If possible, identify deleted e-mails.

26 . (You can identify the following items: Timestamp, From, To, Subject, Body, and Attachment)
[Hint: just examine the OST file only.]

28 . List external storage devices attached to PC.

```
HKLM\SYSTEM\ControlSet001\Enum\USBSTOR> ls
Node has 1 subkeys and 0 values
  key name
  <Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01>

HKLM\SYSTEM\ControlSet001\Enum\USBSTOR>

(...)\4C530012450531101593&0> cat FriendlyName
Value <FriendlyName> of type REG_SZ (1), data length 60 [0x3c]
SanDisk Cruzer Fit USB Device

(...)\4C530012450531101593&0>
Serial Number: 4C530012450531101593

(...)\4C530012450531101593&0> cat CompatibleIDs
Value <CompatibleIDs> of type REG_MULTI_SZ (7), data length 52 [0x34]
USBSTOR\Disk
```

```
USBSTOR\RAW

----------------------------------------------------------------------------

(...)\4C530012550531106501&0> cat FriendlyName
Value <FriendlyName> of type REG_SZ (1), data length 60 [0x3c]
SanDisk Cruzer Fit USB Device

(...)\4C530012550531106501&0>
Serial Number: 4C530012550531106501

----------------------------------------------------------------------------



Plugin [USBSTOR]
===================

[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl  -r /mnt/windows/hdd/Windows/S
ystem32/config/SYSTEM -p usbstor
Launching usbstor v.20141111
usbstor v.20141111
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01 [Tue Mar 24 13:58:32 2015]
  S/N: 4C530012450531101593&0 [Tue Mar 24 13:38:00 2015]
  Device Parameters LastWrite: [Mon Mar 23 18:31:11 2015]
  LogConf LastWrite          : [Mon Mar 23 18:31:10 2015]
  Properties LastWrite       : [Mon Mar 23 18:31:11 2015]
    FriendlyName    : SanDisk Cruzer Fit USB Device
    InstallDate     : Mon Mar 23 18:31:11 2015 UTC
    FirstInstallDate: Mon Mar 23 18:31:11 2015 UTC
  S/N: 4C530012550531106501&0 [Tue Mar 24 13:58:33 2015]
  Device Parameters LastWrite: [Tue Mar 24 13:58:33 2015]
  LogConf LastWrite          : [Tue Mar 24 13:58:32 2015]
  Properties LastWrite       : [Tue Mar 24 13:58:33 2015]
    FriendlyName    : SanDisk Cruzer Fit USB Device
    InstallDate     : Tue Mar 24 13:58:33 2015 UTC
    FirstInstallDate: Tue Mar 24 13:58:33 2015 UTC


Plugin [USBDEVICES]
===================

[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl  -r /mnt/windows/hdd/Windows/S
ystem32/config/SYSTEM -p usbdevices
Launching usbdevices v.20140416
usbdevices v.20140416
(System) Parses Enum\USB key for USB & WPD devices


VID_0781&PID_5571
LastWrite: Tue Mar 24 13:58:31 2015
  SN       : 4C530012550531106501
  LastWrite: Tue Mar 24 19:38:09 2015

VID_0781&PID_5571
LastWrite: Tue Mar 24 13:58:31 2015
```

```
  SN       : 4C530012450531101593
  LastWrite: Tue Mar 24 13:38:00 2015
```

29 . Identify all traces related to ‘renaming’ of files in Windows Desktop.
[Hint: the parent directories of renamed files were deleted and their MFT entries were also overwritten. Therefore, you may not be able to find their full paths.]

To recover all delete data:

```
$> sudo foremost -t png -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost/ -v
$> sudo foremost -t jpg -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost/ -v
$> sudo foremost -t ppt -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost/ -v
$> sudo foremost -t zip -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost/ -v
```

Foremost directory must be empty.

30 . What is the IP address of company’s shared network drive?

In [HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\]:

```
(...)\Windows\CurrentVersion\Explorer\RunMRU> cat MRUList
Value <MRUList> of type REG_SZ (1), data length 6 [0x6]
ba

(...)\Windows\CurrentVersion\Explorer\RunMRU> cat a
Value <a> of type REG_SZ (1), data length 12 [0xc]
cmd\1

(...)\Windows\CurrentVersion\Explorer\RunMRU> cat b
Value <b> of type REG_SZ (1), data length 62 [0x3e]
\\10.11.11.128\secured_drive\1


(...)\Windows\CurrentVersion\Explorer\RunMRU>
```

Other options:
- [HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\]
- [HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\]

33 . List all directories that were traversed in ‘RM#2’.

Traversed...

What are Shellbags?

While shellbags have been available since Windows XP, they have only recently become a popular artifact as examiners are beginning to realize their potential value to an investigation. In a nutshell, shellbags help track views, sizes and positions of a folder window when viewed through Windows Explorer; this includes network folders and removable devices.

Why are Shellbags Important to Digital Forensics Investigations?

One might ask why the position, view, or size of a given folder window is important to forensic investigators. While these properties might not be overly valuable to an investigation, Windows creates a number of additional artifacts when storing these properties in the registry, giving the investigator great insight into the folder, browsing history of a suspect, as well as details for any folder that might no longer exist on a system (due to deletion, or being located on a removable device).

The Key Artifacts That Need to be Found When Investigating Shellbags

For Windows XP, shellbag artifacts are located in the NTUSER.dat registry hive at the following locations:

```
    HKCUSoftwareMicrosoftWindowsShell
    HKCUSoftwareMicrosoftWindowsShellNoRoam
```

For Windows 7 and later, shellbags are also found in the UsrClass.dat hive:

```
    HKCRLocal SettingsSoftwareMicrosoftWindowsShellBags
    HKCRLocal SettingsSoftwareMicrosoftWindowsShellBagMRU
```

Delete files in [RM#2]:

```
.
├── audit.txt
├── bmp
│   └── 00368264.bmp
├── docx
│   ├── 00111528.docx
│   ├── 00120208.docx
│   ├── 00120272.docx
│   ├── 00189080.docx
│   ├── 00201760.docx
│   └── 00202896.docx
├── gif
│   ├── 00192473.gif
│   ├── 00370088.gif
│   ├── 00383240.gif
│   ├── 00389800.gif
│   ├── 00442440.gif
│   ├── 00462760.gif
│   ├── 00510728.gif
│   ├── 00515112.gif
│   └── 00519496.gif
├── jpg
│   ├── 00009466.jpg
│   ├── 00012922.jpg
│   ├── 00012974.jpg
│   ├── 00013010.jpg
│   ├── 00013684.jpg
│   ├── 00014243.jpg
│   ├── 00014614.jpg
│   ├── 00015046.jpg
│   ├── 00015592.jpg
│   ├── 00016143.jpg
│   ├── 00016697.jpg
│   ├── 00022019.jpg
│   ├── 00022095.jpg
│   ├── 00022124.jpg
...
│   ├── 00023683.jpg
│   ├── 00024706.jpg
│   ├── 00483144.jpg
│   ├── 00502376.jpg
│   ├── 00504872.jpg
│   ├── 00506536.jpg
│   └── 00508296.jpg
├── mov
│   ├── 00327048.mov
│   ├── 00336744.mov
│   └── 00338504.mov
├── mp4
│   ├── 00224136.mp4
│   ├── 00247592.mp4
│   └── 00267336.mp4
├── ole
│   ├── 00068640.ole
│   ├── 00111408.ole
│   ├── 00206440.ole
│   └── 00211056.ole
├── png
│   ├── 00010402.png
│   ├── 00012776.png
│   ├── 00012823.png
│   ├── 00013430.png
│   ├── 00016824.png
│   ├── 00016916.png
│   ├── 00016928.png
│   ├── 00016946.png
│   ├── 00178683.png
│   ├── 00178693.png
│   ├── 00178737.png
│   ├── 00179501.png
│   ├── 00181639.png
│   ├── 00181735.png
│   ├── 00183965.png
│   ├── 00184474.png
│   ├── 00184754.png
│   ├── 00184881.png
...
│   ├── 00185008.png
│   ├── 00185302.png
│   ├── 00185427.png
│   ├── 00185988.png
│   ├── 00186697.png
│   ├── 00187489.png
│   ├── 00210508.png
│   ├── 00411176.png
│   ├── 00423240.png
│   ├── 00446920.png
│   └── 00485832.png
├── pptx
│   ├── 00036632.pptx
│   └── 00202000.pptx
├── wav
│   └── 00026017.wav
├── wmv
│   ├── 00284968.wmv
│   ├── 00287496.wmv
│   ├── 00292328.wmv
│   └── 00300712.wmv
├── xlsx
```

```
│   ├── 00071104.xlsx
│   └── 00071304.xlsx
└── zip
    ├── 00026046.zip
    ├── 00026052.zip
    ├── 00026065.zip
    ├── 00026070.zip
    ├── 00026076.zip
    ├── 00026095.zip
    ├── 00026103.zip
    ├── 00026203.zip
    ├── 00026208.zip
    ├── 00026220.zip
    ...
```

34 . List all files that were opened in 'RM#2’.

```
[leviathan3773@latitude:AutomaticDestinations ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/Automa
ticDestinations
[leviathan3773@latitude:AutomaticDestinations ] $ strings 1b4dd67f29cb1962.autom
aticDestinations-ms | grep E:
/E:\
/E:\
E:\RM#1\Secret Project Data\proposal
/E:\
E:\RM#1\Secret Project Data\design
/E:\
E:\Secret Project Data\design\winter_whether_advisory.zip
/E:\
[leviathan3773@latitude:AutomaticDestinations ] $
```

35 . List all directories that were traversed in the company’s network drive.
?? Shell bags..

36 . List all files that were opened in the company’s network drive.

In [HKU\informan\Software\Microsoft\Office\15.0\Excel\File MRU\]:

```
    (...)\Microsoft\Office\15.0\Excel\File MRU> cat Item 1
    Value <Item 1> of type REG_SZ (1), data length 294 [0x126]
    [F00000000][T01D065A7B4C94EE2][O00000000]*\\10.11.11.128\secured_drive\Secre
t Project Data\pricing decision\(secret_project)_pricing_decision.xlsx
```

In [HKU\informan\Software\Microsoft\Office\15.0\PowerPoint\File MRU\]:

```
    (...)\Microsoft\Office\15.0\PowerPoint\File MRU> cat Item 1
    Value <Item 1> of type REG_SZ (1), data length 214 [0xd6]
    [F00000000][T01D065A7CD535A02][O00000000]*V:\Secret Project Data\final\[secr
et_project]_final_meeting.pptx


    (...)\Microsoft\Office\15.0\PowerPoint\File MRU> cat Item 2
    Value <Item 2> of type REG_SZ (1), data length 226 [0xe2]
    [F00000000][T01D065988AED3462][O00000000]*E:\RM#1\Secret Project Data\design
\[secret_project]_design_concept.ppt


    (...)\Microsoft\Office\15.0\PowerPoint\File MRU>
```

37 . Find traces related to cloud services on PC.
(Service name, log files...)

In [HKU\Software\Google\Drive]:

```
\Software\Google\Drive> ls
Node has 0 subkeys and 7 values
  size     type              value name             [value if type DWORD]
    10  1 REG_SZ             <Installed>
    94  1 REG_SZ             <Path>
    30  1 REG_SZ             <FileManagerRestartedVersion>
     4  4 REG_DWORD          <thankyoushown>             1 [0x1]
     4  4 REG_DWORD          <DirectConnection>          0 [0x0]
     4  4 REG_DWORD          <ContextMenuDisabled>       0 [0x0]
     4  4 REG_DWORD          <OverlaysDisabled>          0 [0x0]

\Software\Google\Drive>

Value <Path> of type REG_SZ (1), data length 94 [0x5e]
C:\Users\informant\AppData\Local\Google\Drive\


\Software\Google\Drive>
```

```
[leviathan3773@latitude:Drive ] $ ls
contextmenu64.dll      googledrivesync.exe  Microsoft.VC90.ATL  Microsoft.VC90.M
FC
googledrivesync64.dll  Languages            Microsoft.VC90.CRT  nativeproxy.exe
[leviathan3773@latitude:Drive ] $ pwd
/mnt/windows/boot/Program Files (x86)/Google/Drive

[leviathan3773@latitude:user_default ] $ pwd
/mnt/windows/boot/Users/informant/AppData/Local/Google/Drive/user_default
[leviathan3773@latitude:user_default ] $ ls
cloud_graph  com.google.drive.nativeproxy.json  CrashReports  lockfile  pid  run
_dir  sync_log.log
[leviathan3773@latitude:user_default ] $

[leviathan3773@latitude:Downloads ] $ pwd
/mnt/windows/boot/Users/informant/Downloads
[leviathan3773@latitude:Downloads ] $ ls
desktop.ini  googledrivesync.exe  icloudsetup.exe
```

39 .What files were deleted from Google Drive?
Find the filename and modified timestamp of the file.
[Hint: Find a transaction log file of Google Drive.]

```
[leviathan3773@latitude:user_default ] $ grep happy_holiday sync_log.log
2015-03-23 16:32:35,072 -0400 INFO pid=2576 4004:LocalWatcher    common.aggregat
or:114 --------> Received event RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\inform
ant\\Google Drive\\happy_holiday.jpg', time=1427142755.056, is_dir=False, ino=45
03599627374809L, size=440517L, mtime=1422563714.5256062, parent_ino=844424930207
017L, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_
CONTENT: (False, False)>) None
2015-03-23 16:32:35,072 -0400 INFO pid=2576 4004:LocalWatcher    common.change_b
uffer:1017 Adding event to change buffer: RawEvent(CREATE, path=u'\\\\?\\C:\\Use
rs\\informant\\Google Drive\\happy_holiday.jpg', time=1427142755.056, is_dir=Fal
se, ino=4503599627374809L, size=440517L, mtime=1422563714.5256062, parent_ino=84
4424930207017L, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.
NO_BACKUP_CONTENT: (False, False)>)
2015-03-23 16:32:35,072 -0400 INFO pid=2576 4004:LocalWatcher    common.aggregat
or:114 --------> Received event RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\inform
ant\\Google Drive\\happy_holiday.jpg', time=1427142755.072, is_dir=False, ino=45
03599627374809L, size=440517L, mtime=1422563714.5256062, parent_ino=844424930207
017L, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_
CONTENT: (False, False)>) None
 ...

[leviathan3773@latitude:~ ] $ echo 1427142755.056 | gawk '{print strftime("%c",
$0)}'
lun 23 mar 2015 21:32:35 CET
[leviathan3773@latitude:~ ] $
```

42 . Identify account information for synchronizing Google Drive.

```
[leviathan3773@latitude:user_default ] $ grep -e "@gmail.com" sync_log.log
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   common.service.
user:64 Initializing User instance with new credentials. iaman.informant.persona
l@gmail.com
Email: iaman.informant.personal@gmail.com
2015-03-25 11:21:36,782 -0400 INFO pid=3164 3140:LaunchThreads   common.service.
user:64 Initializing User instance with new credentials. iaman.informant.persona
l@gmail.com
Email: iaman.informant.personal@gmail.com
[leviathan3773@latitude:user_default ] $
```

43 . What a method (or software) was used for burning CD-R?

```
[leviathan3773@latitude:Burn ] $ pwd
/mnt/windows/boot/Users/informant/AppData/Local/Microsoft/Windows/Burn/Burn
```

44 . When did the suspect burn CD-R?
[Hint: It may be one or more times.]

```
Useful information
==================

http://windows.microsoft.com/en-us/windows-vista/burn-a-cd-or-dvd
    > Burning Type 1: Like a USB flash drive
    > Burning Type 2: With a CD/DVD/ player (Mastered)

HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\
> If the last selection is burning type 1, ‘DefaultToMastered’ value will be 0.
> If the last selection is burning type 2, ‘DefaultToMastered’ value will be 1.

(...)\Windows\CurrentVersion\Explorer\CD Burning> ls
Node has 2 subkeys and 4 values
  key name
  <Drives>
  <StagingInfo>
  size     type              value name             [value if type DWORD]
   100  1 REG_SZ             <CD Recorder Drive>
     4  4 REG_DWORD          <DriveIndex>               3 [0x3]
     4  4 REG_DWORD          <DefaultToMastered>        0 [0x0]
     4  4 REG_DWORD          <Auto Close Wizard>        0 [0x0]
```

```
(...)\Windows\CurrentVersion\Explorer\CD Burning> cat DefaultToMastered
Value <DefaultToMastered> of type REG_DWORD (4), data length 4 [0x4]
0x00000000

.

===============================
[leviathan3773@latitude:systemprofile ] $ chntpw -e ntuset.dat

\Control Panel\International\Geo> cat Nation
Value <Nation> of type REG_SZ (1), data length 8 [0x8]
244

In [https://msdn.microsoft.com/en-us/library/windows/desktop/dd374073(v=vs.85).a
spx]
...
0xF0    240 Uganda
0xF1    241 Ukraine
0xF2    242 United Kingdom
0xF4    244 United States
0xF5    245 Burkina Faso
0xF6    246 Uruguay
...
===============================
```

```
[leviathan3773@latitude:IAMAN CD1 ] $ df -hT
S.ficheros                   Tipo     Tamaño Usados  Disp Uso% Montado en
udev                         devtmpfs   3,9G      0  3,9G   0% /dev
tmpfs                        tmpfs      788M   9,5M  779M   2% /run
/dev/sdb1                    ext4       103G    87G   11G  90% /
tmpfs                        tmpfs      3,9G    12M  3,9G   1% /dev/shm
tmpfs                        tmpfs      5,0M   4,0K  5,0M   1% /run/lock
tmpfs                        tmpfs      3,9G      0  3,9G   0% /sys/fs/cgroup
tmpfs                        tmpfs      788M    76K  788M   1% /run/user/1000
/home/leviathan3773/.Private ecryptfs   103G    87G   11G  90% /home/leviathan37
73
/dev/mapper/loop0p1          fuseblk    100M    25M   76M  25% /mnt/windows/boot
/dev/mapper/loop0p2          fuseblk     20G    17G  3,4G  84% /mnt/windows/hdd
/dev/mapper/loop1p1          vfat      1020M   224M  797M  22% /media/leviathan3
773/IAMAN $_@
/dev/loop2                   udf        703M   703M     0 100% /media/leviathan3
773/IAMAN CD1
/dev/sda2                    fuseblk    112G   107G  4,7G  96% /media/leviathan3
773/E062E8AC62E8891C
[leviathan3773@latitude:IAMAN CD1 ] $
```

UDF (Universal Disk Format)

46 . What files were copied from PC to CD-R?
[Hint: Just use PC image only. You can examine transaction logs of the file system for this task.]

First, we extract remove files...

```
$> sudo foremost -t all -i /dev/loop2 -o ~/Escritorio/IAMAN_CD1

[leviathan3773@latitude:IAMAN_CD1 ] $ tree
.
```

```
├── audit.txt
├── docx
├── gif
├── jpg
├── ole
├── png
├── ppt
├── pptx
├── wav
├── xlsx
└── zip

10 directories, 1 file
```

48 . What files were opened from CD-R?

In /mnt/windows/hdd/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations

```
--------------------------------------------------------------
[leviathan3773@latitude:AutomaticDestinations ] $ ls -lat
total 92
drwxrwxrwx 1 root root  8192 mar 25  2015 ..
-rwxrwxrwx 2 root root 17408 mar 25  2015 47bb2136fda3f1ed.automaticDestinations
-ms
drwxrwxrwx 1 root root  4096 mar 25  2015 .
-rwxrwxrwx 2 root root 17920 mar 25  2015 1b4dd67f29cb1962.automaticDestinations
-ms
-rwxrwxrwx 2 root root  3072 mar 25  2015 e36bfc8972e5ab1d.automaticDestinations
-ms
-rwxrwxrwx 2 root root  7680 mar 25  2015 7e4dca80246863e3.automaticDestinations
-ms
-rwxrwxrwx 2 root root 17408 mar 23  2015 4cc9bcff1a772a63.automaticDestinations
-ms
-rwxrwxrwx 2 root root  4608 mar 23  2015 69bacc0499d41c4.automaticDestinations-
ms
--------------------------------------------------------------
```

Clear and Manage Win7 Jump Lists

Windows 7 Jump Lists are stored in these paths. I found this short list of filenames that are associated with specific applications:

PATH: %AppData%\Microsoft\Windows\Recent\AutomaticDestinations

28c8b86deab549a1.automaticDestinations-ms = IE8 Pinned and Recent a7bd71699cd38d1c.automaticDestinations-ms = Word 2010 Pinned and Recent adecfb853d77462a.automaticDestinations-ms = Word 2007 Pinned and Recent a8c43ef36da523b1.automaticDestinations-ms = Word 2003 Pinned and Recent 1b4dd67f29cb1962.automaticDestinations-ms = Windows Explorer Pinned and Recent 918e0ecb43d17e23.automaticDestinations-ms = Notepad Pinned and Recent d7528034b5bd6f28.automaticDestinations-ms = Windows Live Mail Pinned and Recent c7a4093872176c74.automaticDestinations-ms = Paint Shop Pro Pinned and Recent b91050d8b077a4e8.automaticDestinations-ms = Media Center f5ac5390b9115fdb.automaticDestinations-ms = PowerPoint 2007 23646679aaccfae0.automaticDestinations-ms = Adobe Reader 9 aff2ffdd0862ff5c.automaticDestinations-ms = Visual Studio 2012

PATH: %AppData%\Microsoft\Windows\Recent\CustomDestinations

28c8b86deab549a1.customDestinations-ms = IE8 Frequent & Tasks

Useful information:

```
[leviathan3773@latitude:AutomaticDestinations ] $ strings 1b4dd67f29cb1962.autom
aticDestinations-ms | grep D:
/D:\
D:\de\winter_whether_advisory.zip
/D:\
/D:\
/D:\
/D:\
```

In [/mnt/windows/hdd/Users/informant/AppData/Roaming/Microsoft/Windows/Recent]

```
[leviathan3773@latitude:Recent ] $ ls -la *.lnk
-rwxrwxrwx 2 root root   243 mar 24  2015 CD Drive (2).lnk
-rwxrwxrwx 2 root root   243 mar 24  2015 CD Drive.lnk
-rwxrwxrwx 1 root root   555 mar 23  2015 final.lnk
-rwxrwxrwx 2 root root   348 mar 24  2015 Koala.jpg.lnk
-rwxrwxrwx 2 root root   361 mar 24  2015 Penguins.jpg.lnk
-rwxrwxrwx 2 root root  1631 mar 23  2015 pricing decision.lnk
-rwxrwxrwx 2 root root   675 mar 25  2015 Resignation_Letter_(Iaman_Informant).d
ocx.lnk
-rwxrwxrwx 2 root root   602 mar 25  2015 Resignation_Letter_(Iaman_Informant).x
ps.lnk
-rwxrwxrwx 1 root root 11732 mar 23  2015 secret.lnk
-rwxrwxrwx 2 root root 13542 mar 23  2015 [secret_project]_design_concept.lnk
-rwxrwxrwx 2 root root   793 mar 23  2015 [secret_project]_final_meeting.pptx.ln
k
-rwxrwxrwx 2 root root  1952 mar 23  2015 (secret_project)_pricing_decision.xlsx
.lnk
-rwxrwxrwx 2 root root 13475 mar 23  2015 [secret_project]_proposal.lnk
-rwxrwxrwx 2 root root   353 mar 24  2015 Tulips.jpg.lnk
-rwxrwxrwx 2 root root   453 mar 24  2015 winter_whether_advisory.zip.lnk

[leviathan3773@latitude:Recent ] $ strings Koala.jpg.lnk
/D:\
Koala.jpg
IAMAN CD
D:\Koala.jpg
1SPS
[leviathan3773@latitude:Recent ] $ strings Penguins.jpg.lnk
/D:\
Penguins.jpg
IAMAN CD
D:\Penguins.jpg
1SPS
[leviathan3773@latitude:Recent ] $ strings Tulips.jpg.lnk
/D:\
Tulips.jpg
IAMAN CD
D:\Tulips.jpg
1SPS
[leviathan3773@latitude:Recent ] $ strings winter_whether_advisory.zip.lnk
/D:\
WINT#F~U.ZIP
IAMAN CD
D:\de\winter_whether_advisory.zip
1SPS
```

49 . Identify all timestamps related to a resignation file in Windows Desktop.
[Hint: the resignation file is a DOCX file in NTFS file system.]

```
[leviathan3773@latitude:Desktop ] $ stat Resignation_Letter_\(Iaman_Informant\).docx
  Fichero: 'Resignation_Letter_(Iaman_Informant).docx'
  Tamaño: 11893         Bloques: 24         Bloque E/S: 4096   fichero regular
Dispositivo: fc02h/64514d   Nodo-i: 23554       Enlaces: 2
Acceso: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Acceso: 2015-03-24 19:59:30.595570900 +0100
Modificación: 2015-03-24 19:59:30.611171000 +0100
      Cambio: 2015-03-24 19:59:30.611171000 +0100
    Creación: -
[leviathan3773@latitude:Desktop ] $
```

Nothing else

51 . How and when did the suspect print a resignation file?

There are not real printers devices...

The Microsoft XPS Document Writer (MXDW) is a print-to-file driver that enables a Windows application to create XML Paper Specification (XPS) document files on versions of Windows starting with Windows XP with Service Pack 2 (SP2). Using the MXDW makes it possible for a Windows application to save its content as an XPS document without changing any of the application's program code.

In [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\]

```
[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Users/informant/NTUSER.DAT -p printers
Launching printers v.20090223
printers v.20090223
(NTUSER.DAT) Get user's printers

Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts
LastWrite Time: Wed Mar 25 13:06:09 2015

  Microsoft XPS Document Writer (winspool,Ne00:,15,45)
  Fax (winspool,Ne01:,15,45)

Default Printer (via CurrentVersion\Windows): Microsoft XPS Document Writer,winspool,Ne00:
[leviathan3773@latitude:RegRipper2.8 ] $
```

52 . Where are ‘Thumbcache’ files located?

What is "Thumbcache"

If you’ve accidentally downloaded a sensitive image file that can get you into trouble, deleting the file from Windows is just not enough even if you’ve perform a secusure wipe. Forensics people can still retrieve the image from your computer, thanks to the thumbnail caching feature. When you open a folder containing a lot of images, the thumbnail caching feature will greatly improve the time that takes to show the images via thumbnails rather than regenerating them every time you get in to the folder.
Read More: https://www.raymond.cc/blog/what-you-should-know-about-thumbsdb-file/

```
[leviathan3773@latitude:Explorer ] $ ls
ExplorerStartupLog.etl          thumbcache_1024.db  thumbcache_32.db  thumbcache
_idx.db
ExplorerStartupLog_RunOnce.etl  thumbcache_256.db   thumbcache_96.db  thumbcache
_sr.db
[leviathan3773@latitude:Explorer ] $ pwd
/mnt/windows/hdd/Users/informant/AppData/Local/Microsoft/Windows/Explorer
```

53 . Identify traces related to confidential files stored in Thumbcache. (Include ‘256’ only)

file:///home/leviathan3773/Escritorio/cfreds/thumbcache/report256/Report.html

55 . Where are Sticky Note files located?

```
[leviathan3773@latitude:hdd ] $ find . -name "Sticky*"
./Users/informant/AppData/Roaming/Microsoft/Sticky Notes
./Users/informant/AppData/Roaming/Microsoft/Sticky Notes/StickyNotes.snt
```

56 . Identify notes stored in the Sticky Note file.

```
[leviathan3773@latitude:Sticky Notes ] $ strings StickyNotes.snt
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fcha0
rset0 Segoe Print;}{\f1\fnil Segoe Print;}}
{\*\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\tx360\tx720\tx1080\tx14
40\tx1800\tx2160\tx2520\tx2880\tx3240\tx3600\tx3960\tx4320\tx4680\tx5040\tx5400\
tx5760\tx6120\tx6480\tx6840\tx7200\tx7560\tx7920\tx8280\tx8640\tx9000\tx9360\tx9
720\tx10080\tx10440\tx10800\tx11160\tx11520\highlight0\f0\fs22 Tomorrow...\par
\par
Everything will be OK...\par
\par
\lang9\f1\par
[leviathan3773@latitude:Sticky Notes ] $
```

57 . Was the ‘Windows Search and Indexing’ function enabled? How can you identify it?

SearchIndexer.exe is the Windows service that handles indexing of your files for

Windows Search, which fuels the file search engine built into Windows that powers everything
from the Start Menu search box to Windows Explorer, and even the Libraries feature.

You can see this for yourself by simply right-clicking on the process name in the
Task Manager list, and then choosing Go to Service(s) from the menu.

```
Paths:

HKLM\SOFTWARE\Microsoft\Windows Search\
HKLM\SOFTWARE\Microsoft\Windows Search\Databases\Windows (value: FileName)
HKU\informant\Software\Microsoft\Windows Search\
HKLM\SYSTEM\ControlSet001\services\WSearch\ (SearchIndexer service  Start up au
tomatically)
...
================================================================================
====

\Microsoft\Windows Search> cat SystemIndexNormalization
Value <SystemIndexNormalization> of type REG_DWORD (4), data length 4 [0x4]
0x00000001

\Microsoft\Windows Search>

================================================================================
====

If FileName exists, Windows search and indexing are enabled.

\Microsoft\Windows Search\Databases> cd Windows

\Microsoft\Windows Search\Databases\Windows> ls
Node has 0 subkeys and 2 values
  size     type              value name             [value if type DWORD]
   140  1 REG_SZ             <FileName>
   118  1 REG_SZ             <LogPath>

\Microsoft\Windows Search\Databases\Windows> cat FileName
Value <FileName> of type REG_SZ (1), data length 140 [0x8c]
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb


\Microsoft\Windows Search\Databases\Windows> cat LogPath
Value <LogPath> of type REG_SZ (1), data length 118 [0x76]
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\


\Microsoft\Windows Search\Databases\Windows>

================================================================================
====

(...)\Microsoft\Windows Search\Gather\Windows> ls
Node has 1 subkeys and 0 values
  key name
  <SystemIndex>

(...)\Microsoft\Windows Search\Gather\Windows>

================================================================================
====
\ControlSet001\services\WSearch> ls
Node has 0 subkeys and 13 values
  size     type              value name             [value if type DWORD]
    92  1 REG_SZ             <DisplayName>
     4  4 REG_DWORD          <ErrorControl>             1 [0x1]
   102  2 REG_EXPAND_SZ      <ImagePath>
     4  4 REG_DWORD          <Start>                     2 [0x2]
     4  4 REG_DWORD          <Type>                     16 [0x10]
    92  1 REG_SZ             <Description>
    14  7 REG_MULTI_SZ       <DependOnService>
    24  1 REG_SZ             <ObjectName>
     4  4 REG_DWORD          <ServiceSidType>            1 [0x1]
   284  7 REG_MULTI_SZ       <RequiredPrivileges>
     4  4 REG_DWORD          <FailureActionsOnNonCrashFailures> 1       [0x1]
     4  4 REG_DWORD          <DelayedAutoStart>          1 [0x1]
    44  3 REG_BINARY         <FailureActions>

\ControlSet001\services\WSearch> cat DelayedAutoStart
Value <DelayedAutoStart> of type REG_DWORD (4), data length 4 [0x4]
0x00000001

\ControlSet001\services\WSearch>
```

58 . If it was enabled, what is a file path of the ‘Windows Search’ index database?

```
\Microsoft\Windows Search\Databases\Windows> ls
Node has 0 subkeys and 2 values
  size     type              value name             [value if type DWORD]
   140  1 REG_SZ             <FileName>
   118  1 REG_SZ             <LogPath>

\Microsoft\Windows Search\Databases\Windows> cat FileName
Value <FileName> of type REG_SZ (1), data length 140 [0x8c]
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
```

59 . What kinds of data were stored in Windows Search database?

View de database with [ESEDatabaseView]:

```
[leviathan3773@latitude:ESEDatabaseViewer ] $ wine ESEDatabaseView.exe
```

In [SystemIndex_0A (Table ID= 15, 378 Columns)]:

- System_ItemFolderPathDisplay
- System_ItemPathDisplay
- System_Search_Store
- System_ItemNameDisplay
- System_ItemName

60 . Find traces of Internet Explorer usage stored in Windows Search database.
(It should be considered only during a date range between 2015-03-22 and 2015-03-23.)
- Windows.edb
> ‘System_DateModified’ column
> ‘Microsoft_IE_TargetUrl’ column

62 . List the e-mail communication stored in Windows Search database.
(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)
- Windows.edb
> ‘System_ItemPathDisplay’ column
> ‘System_Message_FromName’ column
> ‘System_Message_ToAddress’ column

```
> ‘System_Message_ToName’ column
> ‘System_Message_DateSent’ column
> ‘System_Message_DateReceived’ column
> ‘System_Message_AttachmentNames’ column
> ‘System_Search_AutoSummary’ column
> ‘System_Search_AutoSummary’ column
```

64 . List files and directories related to Windows Desktop stored in Windows Search database.
(Windows Desktop directory: \Users\informant\Desktop\)

```
- Windows.edb
> ‘System_DateCreated’ column
> ‘System_ItemDate’ column
> ‘System_ItemPathDisplay’ column
> ‘System_Search_AutoSummary’ column
```

```
==================================================
DocID              : 471
System_Search_Rank: 707406378
System_Search_GatherTime: 01 D0 66 39 64 03 2B 61
System_Size       : 00 00 00 00 00 F9 F4 C3
System_FileAttributes: 32
System_DateModified: 01 D0 19 4A CD 2C 29 D2
System_DateCreated: 01 D0 66 39 22 E3 14 FE
System_DateAccessed: 01 D0 66 39 22 E3 14 FE
System_Null       :
Microsoft_IE_TargetUrlPath:
System_Photo_GainControlText:
System_Contact_BusinessHomePage:
Microsoft_IE_Title:
System_IsIncomplete:
Microsoft_IE_VisitCount:
System_SDID       :
System_DRM_IsProtected:
System_Contact_SpouseName:
System_DateAcquired:
System_IsFolder   :
System_Message_BccAddress:
System_MIMEType   :
System_IsDeleted  :
System_Message_BccName:
System_Message_CcAddress:
System_Document_Contributor:
System_Search_HitCount:
System_Message_CcName:
System_Search_AccessCount: 8357316
System_ItemFolderPathDisplay: C:\Users\informant\Desktop\S data\Secret Project D
ata\Secret Project Data\design
System_Contact_EmailAddress2:
System_ItemPathDisplay: C:\Users\informant\Desktop\S data\Secret Project Data\Se
cret Project Data\design\[secret_project]_detailed_design.pptx
System_Search_LastIndexedTotalTime:
System_Search_ReverseFileName: xtpp.ngised_deliated_]tcejorp_terces[`
System_Communication_AccountName:
System_ItemUrl    : file:C:/Users/informant/Desktop/S data/Secret Project Data/S
ecret Project Data/design/[secret_project]_detailed_design.pptx
System_IsRead     :
System_Importance :
```

```
System_ContentUrl :
System_Contact_JobTitle:
System_ItemParticipants: company
System_FlagStatus :
System_Contact_OfficeLocation:
System_Message_FromAddress:
....

==================================================
DocID             : 473
System_Search_Rank: 707406378
System_Search_GatherTime: 01 D0 66 39 63 E6 9A DE
System_Size       : 00 00 00 00 00 68 6F 86
System_FileAttributes: 32
System_DateModified: 01 D0 3C AC B1 9B 22 F3
System_DateCreated: 01 D0 66 39 22 FD 44 21
System_DateAccessed: 01 D0 66 39 22 FD 44 21
System_Null       :
Microsoft_IE_TargetUrlPath:
System_Photo_GainControlText:
System_Contact_BusinessHomePage:
Microsoft_IE_Title:
System_IsIncomplete:
Microsoft_IE_VisitCount:
System_SDID       :
System_DRM_IsProtected:
System_Contact_SpouseName:
System_DateAcquired:
System_IsFolder   :
System_Message_BccAddress:
System_MIMEType   :
System_IsDeleted  :
System_Message_BccName:
System_Message_CcAddress:
System_Document_Contributor:
System_Search_HitCount:
System_Message_CcName:
System_Search_AccessCount: 8359420
System_ItemFolderPathDisplay: C:\Users\informant\Desktop\S data\Secret Project D
ata\Secret Project Data\final
System_Contact_EmailAddress2:
System_ItemPathDisplay: C:\Users\informant\Desktop\S data\Secret Project Data\Se
cret Project Data\final\[secret_project]_final_meeting.pptx
System_Search_LastIndexedTotalTime:
System_Search_ReverseFileName: xtpp.gniteem_lanif_]tcejorp_terces[
System_Communication_AccountName:
System_ItemUrl    : file:C:/Users/informant/Desktop/S data/Secret Project Data/S
ecret Project Data/final/[secret_project]_final_meeting.pptx
System_IsRead     :
System_Importance :
System_ContentUrl :
System_Contact_JobTitle:
```

Windows FILETIME to unix, unix to date

```
======================================================================
#include <iostream>
#include <stdlib.h>     /* atol */
```

```
#define SEC_TO_UNIX_EPOCH 11644473600LL
#define WINDOWS_TICK 10000000


using namespace std;

unsigned WindowsTickToUnixSeconds(long long windowsTicks)
{
     return (unsigned)(windowsTicks / WINDOWS_TICK - SEC_TO_UNIX_EPOCH);
}

int main(int argc, char* argv[]){

    if (argc < 1) { cout << "Use " << argv[0] << "<FILETIME>" << endl; return -1
; }

    cout << WindowsTickToUnixSeconds(atol(argv[1])) << endl;
    return 0;
}
======================================================================
```

```
Tricks:
[leviathan3773@latitude:TXTs ] $ echo $((16#01D0663922FD4421))
130716784779936801

[leviathan3773@latitude:TXTs ] $ ./test 130716784779936801 | awk '{ print strfti
me("%c",$0)}'
mar 24 mar 2015 14:47:57 CET
```

----

66 . Where are Volume Shadow Copies stored? When were they created?

```
[leviathan3773@latitude:System Volume Information ] $ pwd
/mnt/windows/hdd/System Volume Information
[leviathan3773@latitude:System Volume Information ] $ ls -lath
total 324M
-rwxrwxrwx 1 root root 2,8M mar 25  2015 Syscache.hve
-rwxrwxrwx 2 root root 256K mar 25  2015 Syscache.hve.LOG1
drwxrwxrwx 1 root root  12K mar 25  2015 ..
drwxrwxrwx 1 root root 4,0K mar 25  2015 .
-rwxrwxrwx 2 root root 320M mar 25  2015 {9b365826-d2ef-11e4-b734-000c29ff2429}{
3808876b-c176-4e48-b7ae-04046e6cc752}
drwxrwxrwx 1 root root 4,0K mar 25  2015 SPP
-rwxrwxrwx 2 root root  64K mar 25  2015 {3808876b-c176-4e48-b7ae-04046e6cc752}
-rwxrwxrwx 1 root root  20K mar 25  2015 tracking.log
-rwxrwxrwx 2 root root    0 mar 25  2015 Syscache.hve.LOG2
-rwxrwxrwx 2 root root    0 mar 25  2015 MountPointManagerRemoteDatabase


[leviathan3773@latitude:~ ] $ sudo vshadowinfo -o 105906176 Escritorio/cfreds/Re
sources/DDs/cfreds_2015_data_leakage_pc.dd
vshadowinfo 20160110

Volume Shadow Snapshot information:
  Number of stores: 1

Store: 1
```

```
  Identifier    : 9b365826-d2ef-11e4-b734-000c29ff2429
  Shadow copy set ID  : 56e43eb5-ac18-4f06-a521-1e17712b7ced
  Creation time   : Mar 25, 2015 14:57:27.293805500 UTC
  Shadow copy ID    : 8f1a2a2d-ce6b-42a5-b92b-f13e65d9c2cb
  Volume size   : 21367881728 bytes
  Attribute flags   : 0x0042000d

[leviathan3773@latitude:~ ] $

[leviathan3773@latitude:~ ] $ sudo vshadowmount -o 105906176 Escritorio/cfreds/R
esources/DDs/cfreds_2015_data_leakage_pc.dd /mnt/vssvolume/
vshadowmount 20160110

[leviathan3773@latitude:~ ] $ sudo ls -la /mnt/vssvolume
total 4
dr-xr-xr-x 2 root root           0 sep 22 12:27 .
drwxr-xr-x 4 root root        4096 sep 22 12:24 ..
-r--r--r-- 1 root root 21367881728 ene  1  1970 vss1
```

Now we mount the [VSS]:

```
[leviathan3773@latitude:mnt ] $ sudo mount -o ro,noexec,nosuid,nodev /mnt/vssvol
ume/vss1 /mnt/vss1logical/
[leviathan3773@latitude:mnt ] $ cd /mnt/vss1logical/
[leviathan3773@latitude:vss1logical ] $ ls
Documents and Settings  MSOCache      PerfLogs     Program Files        Recovery
      System Volume Information  Windows
hiberfil.sys            pagefile.sys  ProgramData  Program Files (x86)  $Recycle
.Bin  Users
[leviathan3773@latitude:vss1logical ] $ df -hT
S.ficheros                    Tipo     Tamaño Usados  Disp Uso% Montado en
udev                          devtmpfs   3,9G      0  3,9G   0% /dev
tmpfs                         tmpfs      788M   9,5M  779M   2% /run
/dev/sdb1                     ext4       103G    81G   17G  83% /
tmpfs                         tmpfs      3,9G   560K  3,9G   1% /dev/shm
tmpfs                         tmpfs      5,0M   4,0K  5,0M   1% /run/lock
tmpfs                         tmpfs      3,9G      0  3,9G   0% /sys/fs/cgroup
tmpfs                         tmpfs      788M    96K  788M   1% /run/user/1000
/home/leviathan3773/.Private ecryptfs   103G    81G   17G  83% /home/leviathan37
73
/dev/mapper/loop0p2           fuseblk     20G    17G  3,4G  84% /mnt/windows/hdd
/dev/mapper/loop1p1           vfat      1020M   224M  797M  22% /mnt/windows/rm2
/dev/loop2                    udf        703M   703M     0 100% /media/leviathan3
773/IAMAN CD
/dev/sda2                     fuseblk    112G   106G  6,3G  95% /media/leviathan3
773/E062E8AC62E8891C
/dev/loop4                    fuseblk     20G    18G  2,8G  87% /mnt/vss1logical
[leviathan3773@latitude:vss1logical ] $
```

67 . Find traces related to Google Drive service in Volume Shadow Copy.
What are the differences between the current system image (of Question 29 ~ 31)
and its VSC?

```
[leviathan3773@latitude:user_default ] $ pwd
/mnt/vss1logical/Users/informant/AppData/Local/Google/Drive/user_default
[leviathan3773@latitude:user_default ] $ ls -lat
total 390
-rwxrwxrwx 1 root root 349702 mar 23  2015 sync_log.log
drwxrwxrwx 1 root root   4096 mar 23  2015 .
```

```
-rwxrwxrwx 2 root root  11264 mar 23  2015 sync_config.db
-rwxrwxrwx 1 root root  20480 mar 23  2015 snapshot.db
drwxrwxrwx 1 root root      0 mar 23  2015 cloud_graph
-rwxrwxrwx 2 root root    294 mar 23  2015 com.google.drive.nativeproxy.json
-rwxrwxrwx 1 root root     46 mar 23  2015 run_dir
drwxrwxrwx 1 root root   4096 mar 23  2015 ..
-rwxrwxrwx 1 root root      4 mar 23  2015 pid
-rwxrwxrwx 2 root root      0 mar 23  2015 lockfile
-rwxrwxrwx 1 root root   3245 mar 23  2015 cacerts
drwxrwxrwx 1 root root      0 mar 23  2015 CrashReports
[leviathan3773@latitude:user_default ] $

Differences:
--------------------------------------------------------------------------------
--------
snapshot.db:                           SQLite 3.x database
sync_config.db:                        SQLite 3.x database
sync_log.log:                          ASCII text, with very long lines, with CRLF l
ine terminators
--------------------------------------------------------------------------------
--------
```

69 . What files were deleted from Google Drive?

```
================================================================================
================================================================
[leviathan3773@latitude:user_default ] $ cat sync_log.log  | egrep "DELETE"

...

2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher    common.aggregat
or:114 --------> Received event RawEvent(DELETE, path=u'\\\\?\\C:\\Users\\inform
ant\\Google Drive\\do_u_wanna_build_a_snow_man.mp3', time=1427143336.964, ino=11
25899906846942L, parent_ino=844424930207017L, affects_gdoc=False, is_cancelled=<
RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, Fal
se)>) None
2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher    common.change_b
uffer:1017 Adding event to change buffer: RawEvent(DELETE, path=u'\\\\?\\C:\\Use
rs\\informant\\Google Drive\\do_u_wanna_build_a_snow_man.mp3', time=1427143336.9
64, ino=1125899906846942L, parent_ino=844424930207017L, affects_gdoc=False, is_c
ancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (
False, False)>)
2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher    common.aggregat
or:114 --------> Received event RawEvent(DELETE, path=u'\\\\?\\C:\\Users\\inform
ant\\Google Drive\\happy_holiday.jpg', time=1427143336.964, ino=4503599627374809
L, parent_ino=844424930207017L, affects_gdoc=False, is_cancelled=<RawEventIsCanc
elledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None
2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher    common.change_b
uffer:1017 Adding event to change buffer: RawEvent(DELETE, path=u'\\\\?\\C:\\Use
rs\\informant\\Google Drive\\happy_holiday.jpg', time=1427143336.964, ino=450359
9627374809L, parent_ino=844424930207017L, affects_gdoc=False, is_cancelled=<RawE
ventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>
)
2015-03-23 16:42:19,369 -0400 INFO pid=2576 3568:Worker-0        common.workers:
188 Worker starting on [ImmutableChange(Direction.UPLOAD, Action.DELETE, ino=112
5899906846942, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'do_u_wa
nna_build_a_snow_man.mp3', parent_ino=844424930207017, affects_gdoc=False, backu
p=Backup.NO_BACKUP_CONTENT, is_cancelled=False, is_priority=False, hash=-1363400
622, _constructor_called=True)]
2015-03-23 16:42:19,385 -0400 INFO pid=2576 2820:Worker-1        common.workers:
```

```
188 Worker starting on [ImmutableChange(Direction.UPLOAD, Action.DELETE, ino=450
3599627374809, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'happy_h
oliday.jpg', parent_ino=844424930207017, affects_gdoc=False, backup=Backup.NO_BA
CKUP_CONTENT, is_cancelled=False, is_priority=False, hash=481398202, _constructo
r_called=True)]
2015-03-23 16:42:20,072 -0400 INFO pid=2576 2820:Worker-1        common.workers:
199 Worker successfully completed [ImmutableChange(Direction.UPLOAD, Action.DELE
TE, ino=4503599627374809, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', nam
e=u'happy_holiday.jpg', parent_ino=844424930207017, affects_gdoc=False, backup=B
ackup.NO_BACKUP_CONTENT, is_cancelled=False, is_priority=False, hash=481398202,
_constructor_called=True)]
2015-03-23 16:42:20,072 -0400 INFO pid=2576 2820:Worker-1        common.change_b
uffer:276 Removing entry from change buffer: ChangeBufferEntry(state=IN_PROGRESS
, fschange=ImmutableChange(Direction.UPLOAD, Action.DELETE, ino=4503599627374809
, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'happy_holiday.jpg',
parent_ino=844424930207017, affects_gdoc=False, backup=Backup.NO_BACKUP_CONTENT,
 is_cancelled=False, is_priority=False, hash=481398202, _constructor_called=True
), raw_event=ImmutableRawEvent(op=DELETE, path=\\?\C:\Users\informant\Google Dri
ve\happy_holiday.jpg, time=1427143336.96, is_dir=None, ino=4503599627374809, siz
e=None, old_path=None, new_ino=None, mtime=None, parent_ino=844424930207017, aff
ects_gdoc=False, is_cancelled=RawEventIsCancelledFlag.FALSE, old_parent_ino=None
, backup=Backup.NO_BACKUP_CONTENT, _hash_code=1349549055), sequence_number=7)
2015-03-23 16:42:22,709 -0400 INFO pid=2576 3568:Worker-0        common.workers:
199 Worker successfully completed [ImmutableChange(Direction.UPLOAD, Action.DELE
TE, ino=1125899906846942, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', nam
e=u'do_u_wanna_build_a_snow_man.mp3', parent_ino=844424930207017, affects_gdoc=F
alse, backup=Backup.NO_BACKUP_CONTENT, is_cancelled=False, is_priority=False, ha
sh=-1363400622, _constructor_called=True)]
2015-03-23 16:42:22,709 -0400 INFO pid=2576 3568:Worker-0        common.change_b
uffer:276 Removing entry from change buffer: ChangeBufferEntry(state=IN_PROGRESS
, fschange=ImmutableChange(Direction.UPLOAD, Action.DELETE, ino=1125899906846942
, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'do_u_wanna_build_a_s
now_man.mp3', parent_ino=844424930207017, affects_gdoc=False, backup=Backup.NO_B
ACKUP_CONTENT, is_cancelled=False, is_priority=False, hash=-1363400622, _constru
ctor_called=True), raw_event=ImmutableRawEvent(op=DELETE, path=\\?\C:\Users\info
rmant\Google Drive\do_u_wanna_build_a_snow_man.mp3, time=1427143336.96, is_dir=N
one, ino=1125899906846942, size=None, old_path=None, new_ino=None, mtime=None, p
arent_ino=844424930207017, affects_gdoc=False, is_cancelled=RawEventIsCancelledF
lag.FALSE, old_parent_ino=None, backup=Backup.NO_BACKUP_CONTENT, _hash_code=2798
86661), sequence_number=6)
2015-03-23 16:42:23,411 -0400 INFO pid=2576 3496:Batcher         common.batcher:
846 Batcher Stats = file_count = Counter({_COUNT_KEY(direction=_UploadDirectionT
ype(Direction.UPLOAD), action=_FSChangeActionType(Action.DELETE), batch=False, s
uccessful=True): 2}), byte_count = Counter(), batch_operation_count = Counter(),
 process_seconds = Counter({_COUNT_KEY(direction=_UploadDirectionType(Direction.
UPLOAD), action=_FSChangeActionType(Action.DELETE), batch=False, successful=True
): 4.025000333786011}), duration seconds = 4 (start_time = 1427143339, end_time
= 1427143343)
[leviathan3773@latitude:user_default ] $
================================================================================
================================================================

[leviathan3773@latitude:user_default ] $ awk -F"," '/DELETE/ { print $5,$6 }' sy
nc_log.log
 ...

 path=u'\\\\?\\C:\\Users\\informant\\Google Drive'  name=u'do_u_wanna_build_a_sn
ow_man.mp3'
 path=u'\\\\?\\C:\\Users\\informant\\Google Drive'  name=u'happy_holiday.jpg'
 path=u'\\\\?\\C:\\Users\\informant\\Google Drive'  name=u'happy_holiday.jpg'
 ...
 path=u'\\\\?\\C:\\Users\\informant\\Google Drive'  name=u'do_u_wanna_build_a_sn
ow_man.mp3'

[leviathan3773@latitude:user_default ] $
```

70 . Find deleted records of cloud_entry table inside snapshot.db from VSC.
(Just examine the SQLite database only. Let us suppose that a text based log file was wiped.)
[Hint: DDL of cloud_entry table is as follows.]

```
CREATE TABLE cloud_entry
(doc_id TEXT, filename TEXT, modified INTEGER, created INTEGER, acl_role INTEGER
,
doc_type INTEGER, removed INTEGER, size INTEGER, checksum TEXT, shared INTEGER,
resource_type TEXT, PRIMARY KEY (doc_id));
```

http://www.sqlite.org/fileformat2.htm

77 . Why can’t we find Outlook’s e-mail data in Volume Shadow Copy?

Because were excluded by the following snapshot configuration

```
================================================================================
============================================================
[leviathan3773@latitude:user_default ] $ strings snapshot.db
SQLite format 3
/indexcloud_relations_parent_doc_id_idxcloud_relations
CREATE INDEX cloud_relations_parent_doc_id_idx on cloud_relations (parent_doc_id
)
Otablecloud_relationscloud_relations
CREATE TABLE cloud_relations (child_doc_id TEXT, parent_doc_id TEXT, UNIQUE (chi
ld_doc_id, parent_doc_id), FOREIGN KEY (child_doc_id) REFERENCES cloud_entry(doc
_id), FOREIGN KEY (parent_doc_id) REFERENCES cloud_entry(doc_id))=
indexsqlite_autoindex_cloud_relations_1cloud_relations
Utablecloud_entrycloud_entry
CREATE TABLE cloud_entry (doc_id TEXT, filename TEXT, modified INTEGER, created
INTEGER, acl_role INTEGER, doc_type INTEGER, removed INTEGER, size INTEGER, chec
ksum TEXT, shared INTEGER, resource_type TEXT, PRIMARY KEY (doc_id))5
indexsqlite_autoindex_cloud_entry_1cloud_
0Bz0ye6gXtiZaVl8yVU5mWHlGbWcdo_u_wanna_build_a_snow_man.mp3T
xmho
2c4553f99533d85adb104b3a5c38521afile
0Bz0ye6gXtiZaakx6d3R3c0JmM1Uhappy_holiday.jpgT
0c77d6a2704155dbfdf29817769b7478file
rootrootfolder
0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
!0Bz0ye6gXtiZaakx6d3R3c0JmM1U
  root
0Bz0ye6gXtiZaVl8yVU5mWHlGbWcroot
0Bz0ye6gXtiZaakx6d3R3c0JmM1Uroot
0Bz0ye6gXtiZaVl8yVU5mWHlGbWcroot
% 0Bz0ye6gXtiZaakx6d3R3c0JmM1Uroot
root
root
0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
 0Bz0ye6gXtiZaakx6d3R3c0JmM1U
Utablecloud_entrycloud_entry
CREATE TABLE cloud_entry (doc_id TEXT, filename TEXT, modified INTEGER, created
INTEGER, acl_role INTEGE
Utablecloud_entrycloud_entry
CREATE TABLE cloud_entry (doc_id TEXT, filename TEXT, modified INTEGER, created
INTEGER, acl_role INTEGER, doc_type INTEGER, removed INTEGER, size INTEGER, chec
ksum TEXT, shared INTEGER, resource_type TEXT, PRIMARY KEY (doc_id))5
indexsqlite_autoindex_cloud_entry_1cloud_entry
Otablecloud_relationscloud_relations
CREATE TABLE cloud_relations (child_doc_id TEXT, parent_doc_id TEXT, UNIQUE (chi
ld_doc_id, parent_doc_id), FOREIGN KEY (child_doc_id) REFERENCES cloud_entry(doc
_id), FOREIGN KEY (parent_doc_id) REFERENCES cloud_entry(doc_id))=
indexsqlite_autoindex_cloud_relations_1cloud_relations
/indexcloud_relations_parent_doc_id_idxcloud_relations
CREATE INDEX cloud_relations_parent_doc_id_idx on cloud_relations (parent_doc_id
)
do_u_wanna_build_a_snow_man.mp3A
#T(2c4553f99533d85adb104b3a5c38521aho
happy_holiday.jpgA
0c77d6a2704155dbfdf29817769b7478
\\?\C:\Users\informant\Google Drive
tablemappingmapping
CREATE TABLE mapping (inode_number INTEGER, doc_id TEXT, UNIQUE (inode_number),
FOREIGN KEY (inode_number) REFERENCES local_entry(inode_number), FOREIGN KEY (do
c_id) REFERENCES cloud_entry(doc_id))-
indexsqlite_autoindex_mapping_1mapping
tablelocal_
+indexcloud_relations_child_doc_id_idxcloud_relations
CREATE INDEX cloud_relations_child_doc_id_idx on cloud_relations (child_doc_id)
tablelocal_entrylocal_entry CREATE TABLE local_entry (inode_number INTEGER, file
name TEXT, modified INTEGER, checksum TEXT, size INTEGER, PRIMARY KEY (inode_num
ber))
tablelocal_relationslocal_relations
CREATE TABLE local_relations (child_inode_number INTEGER, parent_inode_number IN
TEGER, UNIQUE (child_inode_number), FOREIGN KEY (parent_inode_number) REFERENCES
 local_entry(inode_number), FOREIGN KEY (child_inode_number) REFERENCES local_en
try(inode_number))=
indexsqlite_autoindex_local_relations_1local_relations
0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
0Bz0ye6gXtiZaakx6d3R3c0JmM1U
%)root
0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
!0Bz0ye6gXtiZaakx6d3R3c0JmM1U
  root
3tableoverlay_statusoverlay_status
CREATE TABLE overlay_status (path TEXT, overlay_status INTEGER, PRIMARY KEY (pat
h));
indexsqlite_autoindex_overlay_status_1overlay_status
indexmapping_inode_number_idxmapping
CREATE INDEX mapping_inode_number_idx on mapping (inode_number)
Gindexlocal_relations_parent_inode_number_idxlocal_relations
CREATE INDEX local_relations_parent_inode_number_idx on local_relations (parent_
inode_number)
tablemappingmapping
CREATE TABLE mapping (inode_number INTEGER, doc_id TEXT, UNIQUE (inode_number),
FOREIGN KEY (inode_number) REFERENCES local_entry(inode_number), FOREIGN KEY (do
c_id) REFERENCES cloud_entry(doc_id))-
indexsqlite_autoindex_mapping_1mapping
sindexmapping_doc_id_idxmapping
CREATE INDEX mapping_doc_id_idx on mapping (doc_id)
\\?\C:\Users\informant\Google Drive\happy_holiday.jpg
  \\?\C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3
```

```
w \\?\C:\Users\informant\Google Drive\happy_holiday.jpgG
  \\?\C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3
================================================================================
============================================================
```

Database format (Bytes):
  [http://www.sqlite.org/fileformat2.html]

With this forensic tool [https://github.com/mdegrazia/SQLite-Deleted-Records-Parser]:

Use:

```
$> sudo python sqlparse_v1.3.py  -f /mnt/vss1logical/Users/informant/AppData/Loc
al/Google/Drive/user_default/snapshot.db -o report.tsv
```

Epic fail to read Windoze registers (mount readonly):

```
[leviathan3773@latitude:config ] $ chntpw -e SYSTEM
chntpw version 1.00 140201, (c) Petter N Hagen
openHive(SYSTEM) failed: Read-only file system, trying read-only
openHive(): read error: : Read-only file system
chntpw: Unable to open/read a hive, exiting..
[leviathan3773@latitude:config ] $
```

Try...

```
[leviathan3773@latitude:~ ] $ sudo mount -o nodev,noexec,nosuid /mnt/vssvolume/v
ss1 /mnt/vss1logical/

ntfs-3g-mount: mount failed: Permiso denegado
[leviathan3773@latitude:~ ] $ sudo mount -o ro,nodev,noexec,nosuid /mnt/vssvolum
e/vss1 /mnt/vss1logical/
```

Solution??

78 . Examine ‘Recycle Bin’ data in PC.

The SID of ‘informant’ account is 1000.

[.dll] files:

biblioteca de vínculos dinámicos (DLL).
....
El uso de archivos DLL ayuda a promover el diseño modular de código, la
reutilización de código, uso eficaz de la memoria y espacio en disco reducido.
Por lo tanto, el sistema operativo y los programas se cargan más rápido, se
ejecutan más rápidamente y tienen menos espacio en disco en el equipo.

Cuando un programa utiliza un archivo DLL, un problema que se denomina
dependencia puede provocar que el programa no se ejecute. Cuando un
programa utiliza un archivo DLL, se crea una dependencia. Si otro programa
sobrescribe y rompe esta dependencia, entonces no es posible ejecutar
correctamente el programa original.

Con la introducción de la de Microsoft.NET Framework, se han eliminado
la mayoría de los problemas de dependencia mediante el uso de ensamblados.
....

```
Foremost started at Thu Sep 22 14:23:34 2016
```

```
Invocation: foremost -t all -i /dev/loop4 -o /home/leviathan3773/Escritorio/cfre
ds/RecycleBinSnapshot/
Output directory: /home/leviathan3773/Escritorio/cfreds/RecycleBinSnapshot
Configuration file: /etc/foremost.conf
------------------------------------------------------------------

File: /dev/loop4
Start: Thu Sep 22 14:23:34 2016
Length: 19 GB (21367881728 bytes)

Num  Name (bs=512)         Size  File Offset   Comment
[leviathan3773@latitude:RecycleBinSnapshot ] $ cat audit.txt | awk '$6 ~ /2015/
&& $2 !~ /.dll/ { print $0 }'
11400:  02911312.exe        99 KB    1490591744    01/22/2015 01:07:56
11407:  02986960.exe       784 KB    1529323520    03/14/2015 08:41:26
11408:  03022480.exe         1 MB    1547509760    03/14/2015 07:40:46
13935:  03509648.exe       781 KB    1796939776    02/20/2015 00:51:50
13938:  03518144.exe        44 KB    1801289728    01/22/2015 01:21:27
13954:  03567712.exe       844 KB    1826668544    01/22/2015 01:07:44
13955:  03579000.exe        44 KB    1832448000    01/22/2015 01:17:55
13957:  03649824.exe        44 KB    1868709888    01/22/2015 01:17:52
17801:  05779072.exe       844 KB    2958884864    01/22/2015 01:07:44
20363:  06968829.exe       220 KB    3568040448    01/22/2015 01:11:17
20422:  07088224.exe       844 KB    3629170688    01/22/2015 01:07:44
21165:  07623456.exe       216 KB    3903209472    02/20/2015 01:59:49
21174:  07728128.exe         1 MB    3956801536    03/14/2015 07:40:46
21175:  07732664.exe       458 KB    3959123968    02/20/2015 01:35:47
21294:  08131208.exe       113 KB    4163178496    02/20/2015 01:56:54
24418:  09522576.exe        69 KB    4875558912    02/19/2015 22:18:57
25327:  11324432.exe        99 KB    5798109184    01/22/2015 01:07:56
33371:  14572216.exe       640 KB    7460974592    03/14/2015 08:10:44
36408:  17019728.exe       220 KB    8714100736    01/22/2015 01:11:17
53240:  24644480.exe         4 KB    12617973760   01/22/2015 01:07:22
58427:  27236143.exe        11 KB    13944905216   02/19/2015 22:21:37
58480:  27353675.exe         1 MB    14005082027   01/12/2015 18:55:49
59733:  27975587.exe         1 MB    14323500971   01/12/2015 18:55:49
65385:  28776167.exe        11 KB    14733397504   02/19/2015 22:21:37
65387:  28850751.exe        11 KB    14771584512   02/19/2015 22:21:37
65449:  29673760.exe       784 KB    15192965319   03/14/2015 08:41:26
65450:  29675341.exe       640 KB    15193774607   03/14/2015 08:10:44
```

79 . What actions were performed for anti-forensics on PC at the last day '2015-03-25'?
Read this document and list all evinces...

80 . Recover deleted files from USB drive ‘RM#2’.

See [/home/leviathan3773/Escritorio/cfreds/recoveryPhotorec/rm2] and
(more results) [/home/leviathan3773/Escritorio/cfreds/recoveryForemost/rm2/test2]

81 . What actions were performed for anti-forensics on USB drive ‘RM#2’?
[Hint: this can be inferred from the results of Question 53.]

Quick format for deleting data...

83 . What files were copied from PC to USB drive ‘RM#2’?

- Inference from the results of deleted data recovery in Question 53.
- Inference from the results of traversed files/directories in Question 25 and 26.

84 . Recover hidden files from the CD-R ‘RM#3’.

See [/home/leviathan3773/Escritorio/cfreds/recoveryForemost/IAMAN_CD1]

How to determine proper filenames of the original files prior to renaming tasks?

- Metadata based data recovery
> If this task is possible, it may be good for analyst.
> With this method, we may be able to identify renamed filenames.
> So, additional process is needed for determining original filenames.

```
[leviathan3773@latitude:docx ] $ exiftool *.docx | awk '/========/ {print $0}
> /Title\s/ { print "Title", $3 } /Create Date/ { print "Create Date: " $4,$5 }
/^Modify Date/ { print "Modify Date:"$4,$5}'
```

86 . What actions were performed for anti-forensics on CD-R ‘RM#3’?

View all document and extract it.

(1) Formatting CD-R (Burning Type 1: Like a USB flash drive)
(2) Copying confidential files and some meaningless files to CD-R
(3) Deleting confidential files from CD-R for hiding them

87 . Create a detailed timeline of data leakage processes.
- Behavior of the suspect
> 2015-03-22: Normal business works (installation and configuration of apps)
> 2015-03-23: Transferring sample confidential data through the internet
> 2015-03-24: Copying confidential data to storage devices
> 2015-03-25: Trying to do anti-forensics and take storage devices out

View this document and extract it.

88 . List and explain methodologies of data leakage performed by the suspect.

View this document and extract it.

89 . Create a visual diagram for a summary of results.

View this document and extract it.