

<http://www.digitalforensicssolutions.com/Scalpel/>

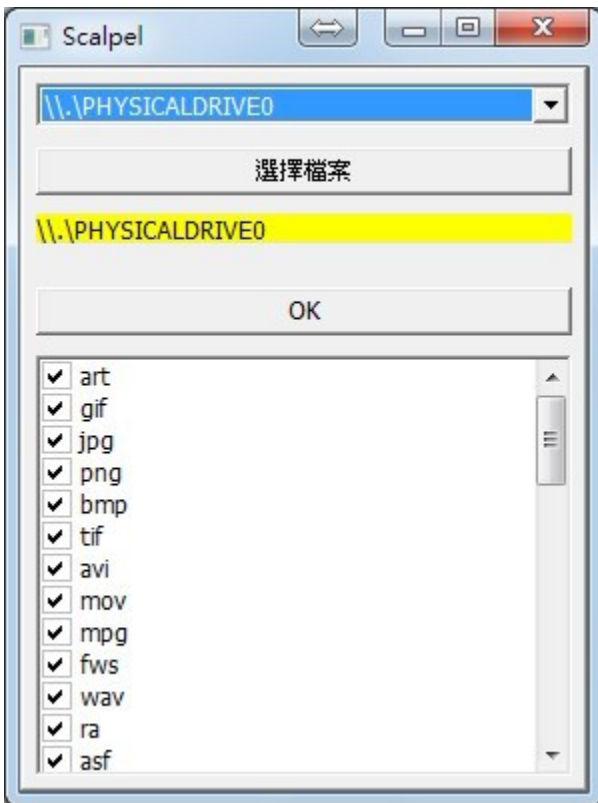
?File system ?????.Rstudio ?????????????,???Block??????.
 ?????????.

Scalpel ??? file carver recovery ?????? ,???file header ?block ??.
 ??????Rstudio ??????
 ??Scalpel ??command ??? ???? ???? ?

????????????????????
 ???????? (???GPL ??)

???? ?? ZIP ?..?

- 1.??Sources IMG ????????
- 2.???????????????
- 3.?????? (????????) ???????



```
#-*- coding: UTF-8 -*-
# Scalpel GUI 0.1
# Code by OSSLab thx .
```

```
import wx
```

```
import os
import wmi
import subprocess
```

```
ext = """"# art y 150000 \\x4a\\x47\\x04\\x0e \\xcf\\xc7\\xcb
# art y 150000 \\x4a\\x47\\x03\\x0e \\xd0\\xcb\\x00\\x00
# gif y 5000000 \\x47\\x49\\x46\\x38\\x37\\x61 \\x00\\x3b
# gif y 5000000 \\x47\\x49\\x46\\x38\\x39\\x61 \\x00\\x00\\x3b
# jpg y 200000000 \\xff\\xd8\\xff\\xe0\\x00\\x10 \\xff\\xd9
# jpg y 200000000 \\xff\\xd8\\xff\\xe1 \\xff\\xd9
# png y 20000000 \\x50\\x4e\\x47? \\xff\\xfc\\xfd\\xfe
# bmp y 100000 BM??\\x00\\x00\\x00
# tif y 200000000 \\x49\\x49\\x2a\\x00
# tif y 200000000 \\x4D\\x4D\\x00\\x2A
# avi y 50000000 RIFF????AVI
# mov y 10000000 ????moov
# mov y 10000000 ????mdat
# mov y 10000000 ????widev
# mov y 10000000 ????skip
# mov y 10000000 ????free
# mov y 10000000 ????idsc
# mov y 10000000 ????pckg
# mpg y 50000000 \\x00\\x00\\x01\\xba \\x00\\x00\\x01\\xb9
# mpg y 50000000 \\x00\\x00\\x01\\xb3 \\x00\\x00\\x01\\xb7
# fws y 4000000 FWS
# wav y 200000 RIFF????WAVE
# ra y 1000000 .RMF
# ra y 1000000 \\x2e\\x72\\x61\\xfd
# asf y 8000000
\\x30\\x26\\xB2\\x75\\x8E\\x66\\xCF\\x11\\xA6\\xD9\\x00\\xAA\\x00\\x62\\xCE\\x6C
# wmv y 20000000
\\x30\\x26\\xB2\\x75\\x8E\\x66\\xCF\\x11\\xA6\\xD9\\x00\\xAA\\x00\\x62\\xCE\\x6C
# wma y 8000000 \\x30\\x26\\xB2\\x75 \\x00\\x00\\x00\\xFF
# wma y 8000000 \\x30\\x26\\xB2\\x75 \\x52\\x9A\\x12\\x46
# mp3 y 8000000 \\xFF\\xFB??\\x44\\x00\\x00
# mp3 y 8000000 \\x57\\x41\\x56\\x45 \\x00\\x00\\xFF\\
# mp3 y 8000000 \\xFF\\xFB\\xD0\\ \\xD1\\x35\\x51\\xCC\\
# mp3 y 8000000 \\x49\\x44\\x33\\
# mp3 y 8000000 \\x4C\\x41\\x4D\\x45\\
# doc y 10000000 \\xd0\\xcf\\x11\\xe0\\xa1\\xb1\\x1a\\xe1\\x00\\x00
\\xd0\\xcf\\x11\\xe0\\xa1\\xb1\\x1a\\xe1\\x00\\x00 NEXT
# doc y 10000000 \\xd0\\xcf\\x11\\xe0\\xa1\\xb1
# pst y 500000000 \\x21\\x42\\x4e\\xa5\\x6f\\xb5\\xa6
# ost y 500000000 \\x21\\x42\\x44\\x4e
# dbx y 10000000 \\xcf\\xad\\x12\\xfe\\xc5\\xfd\\x74\\x6f
# idx y 10000000 \\x4a\\x4d\\x46\\x39
# mbx y 10000000 \\x4a\\x4d\\x46\\x36
# wpc y 1000000 ?WPC
# htm n 50000 <html </html>
# pdf y 5000000 %PDF %EOF\\x0d REVERSE
```

```

# pdf y 5000000 %PDF %EOF\ \x0a REVERSE
# mail y 500000 \ \x41\ \x4f\ \x4c\ \x56\ \x4d
# rpm y 1000000 \ \xed\ \xab
# dat y 4000000 regf
# dat y 4000000 CREG
# zip y 10000000 PK\ \x03\ \x04 \ \x3c\ \xac
# rar y 10000000 Rar!
# java y 1000000 \ \xca\ \xfe\ \xba\ \xbe
# max y 1000000 \ \x56\ \x69\ \x47\ \x46\ \x6b\ \x1a\ \x00\ \x00\ \x00\ \x00
\ \x00\ \x00\ \x05\ \x80\ \x00\ \x00
# pins y 8000 \ \x50\ \x49\ \x4e\ \x53\ \x20\ \x34\ \x2e\ \x32\ \x30\ \x0d
# vbox y 10000000000
<<<????????????????????????????????????????????????????????????\ \x00\ \x7f\ \x10\ \xda\ \xbe
# tgz y 2000000 \ \x1f\ \x8b\ \x08\ \x08
# 7z y 2147483648 \ \x37\ \x7a\ \xbc\ \xaf\ \x27\ \x1c
# ogg y 15728640 x4fx67x67x53x00x02 x4fx67x67x53x00x02 NEXT
# lnk y 4000
\ \x4c\ \x00\ \x00\ \x00\ \x01\ \x14\ \x02\ \x00\ \x00\ \x00\ \x00\ \x00\ \xc0\ \x00\ \x00\ \x00\ \x00\ \x00\ \x46
# shd y 2000 \ \x67\ \x49\ \x00\ \x00
# shd y 2000 \ \x4B\ \x49\ \x00\ \x00
# blend y 1000000000 BLENDER_v ENDB
# mus y 1000000000 ENIGMA\ \x20BINARY\ \x20FILE \ \x13\ \x00\ \x06\ \x00\ \x00\ \x00
# dat y 8192 DynamicDictionary
# amr y 65535 #!AMR
# plist y 4096 <plist </plist
# email y 4096 From:"""

```

```
class MyApp(wx.App):
```

```

    #outputWindowClass = LogWindow
    def __init__(self, redirect=True):
        wx.App.__init__(self, redirect)

```

```
class main(wx.Frame):
```

```

    def __init__(self, parent, id, title, size):
        wx.Frame.__init__(self, parent, id, title, size = size)
        self._main()

```

```
def CreateElement(self):
```

```

    # initial UI
    panel = wx.Panel(self, -1, style=wx.RAISED_BORDER)

```

```
    # Get physical disk driver
```

```

    c = [x.Name for x in wmi.WMI().query("SELECT * FROM Win32_DiskDrive")]
    self.phyDrivers = wx.Choice(panel, -1, choices = c)
    self.phyDrivers.SetSelection(0)

```

```

# Create selecti image button
self.file = wx.Button(panel, -1, u"????")
# Create Start scalpel button
self.start = wx.Button(panel, -1, u"OK")

# choice options
global ext
c = []
for i in ext.split("# ")[1:]:
    __ = i.split(" ", 1)[0]
    if __ not in c:
        c.append( __ )

self.checkList = wx.CheckListBox(panel, -1, size=wx.DefaultSize, choices=c)
self.checkList.SetChecked(range(len(c)))

# Create label
self.label = wx.StaticText(panel, -1, self.phyDrivers.GetStringSelection())
self.label.SetBackgroundColour('yellow')

# Setting UI
box = wx.BoxSizer(wx.VERTICAL)
box.Add(self.phyDrivers, 0, wx.ALL|wx.EXPAND, 5)
box.Add(self.file, 0, wx.ALL|wx.EXPAND, 5)
box.Add(self.label, 0, wx.ALL|wx.EXPAND, 5)
box.Add(wx.StaticLine(panel, -1), 0, wx.ALL, 5)
box.Add(self.start, 0, wx.ALL|wx.EXPAND, 5)
box.Add(self.checkList, 2, wx.ALL|wx.EXPAND, 5)

# Binding event
self.phyDrivers.Bind(wx.EVT_CHOICE, self.OnChoice)
self.start.Bind(wx.EVT_BUTTON, self.OnStart)
self.file.Bind(wx.EVT_BUTTON, self.OnSelectFile)

panel.SetSizer(box)

def OnChoice(self, evt):
    self.label.SetLabel( evt.GetString() )

def OnSelectFile(self, evt):
    dlg = wx.FileDialog(
        self, message="Choose a image file",
        defaultDir=os.getcwd(),
        defaultFile="",
        #wildcard=wildcard,
        style=wx.OPEN | wx.MULTIPLE | wx.CHANGE_DIR
    )

    if dlg.ShowModal() == wx.ID_OK:
        paths = dlg.GetPaths()

```

```

    path = paths[0]
else:
    path = None
dlg.Destroy()

if path:
    self.label.SetLabel( path )

def OnStart(self, evt):
    # generate scalpel.conf
    global ext
    buf = []
    __ = ext.split("# ")
    for i in self.checkList.GetCheckedStrings():
        [buf.append(x) for x in ext.split("# ") if x.startswith(str(i))]

    with open("./scalpel.conf", "wb") as fp:
        fp.write( "".join(buf) )

    dlg = wx.DirDialog(self, "Choose output directory:",
                      style=wx.DD_DEFAULT_STYLE
                      #| wx.DD_DIR_MUST_EXIST
                      #| wx.DD_CHANGE_DIR
                      )

    if dlg.ShowModal() == wx.ID_OK:
        directory = dlg.GetPath()
    else:
        directory = None
    dlg.Destroy()

    if directory:
        img = self.label.GetLabelText()
        subprocess.call( "bin\\scalpel.exe -v -o %s %s" % (directory, img) )
        subprocess.call("rundll32.exe user32,MessageBoxA aaa")

def _main(self):
    # Create Buttons & Texts
    self.CreateElement()

    self.Centre()
    self.Show()

if __name__ == "__main__":
    app = MyApp(redirect=True)

    frame = main(None, -1, "Scalpel", (300, 400))
    app.MainLoop()

```