



Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number – 11 – Packet Analyzing with scap

February 23, 2019

University of Colombo School of Computing

Table of Contents

Study Number – 11 – Packet Analyzing with scap 1

 Problem3

 Approach.....3

 Conclusion 14

Problem

Setup

- Download folder from LMS
- docker build . -t scapy
- docker -it -p 8888:8888 scapy:latest
- You can access the Jupyter notebook from flowing link:
 - [http://\[Docker IP\]:8888/](http://[Docker IP]:8888/)
- Password: 123

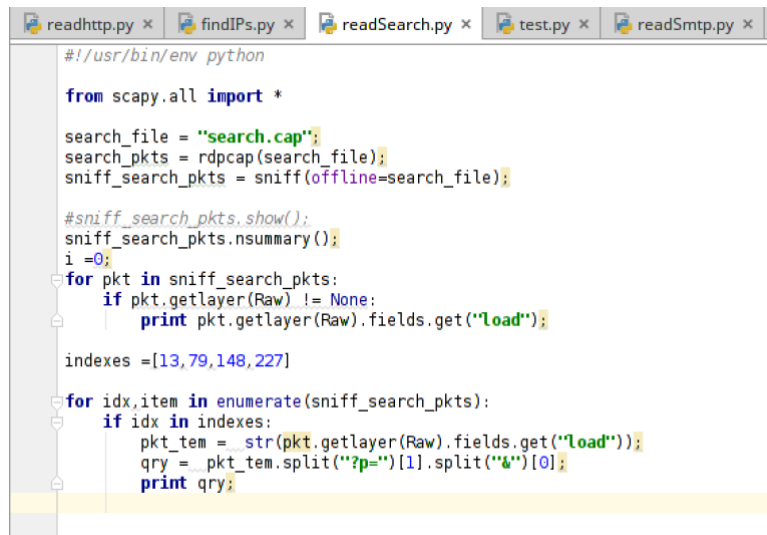
Tasks

1. Analyze Search Search Traffic
 - Find search engine name and Search queries
2. Analyze Site Visitors
 - Find the IP's of site visitors
3. Analyze Email
 - Find Email Providers, Email Addresses, Participants, Passwords, Email Client, Attachments,

Approach

Tasks

1. Analyze Search Search Traffic
 - Find search engine name and Search queries



```
#!/usr/bin/env python

from scapy.all import *

search_file = "search.cap";
search_pkts = rdpcap(search_file);
sniff_search_pkts = sniff(offline=search_file);

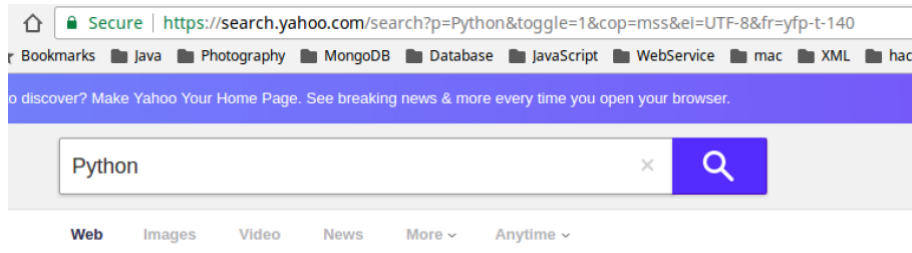
#sniff_search_pkts.show();
sniff_search_pkts.nsummary();
i = 0;
for pkt in sniff_search_pkts:
    if pkt.getlayer(Raw) != None:
        print pkt.getlayer(Raw).fields.get("load");

indexes = [13, 79, 148, 227]

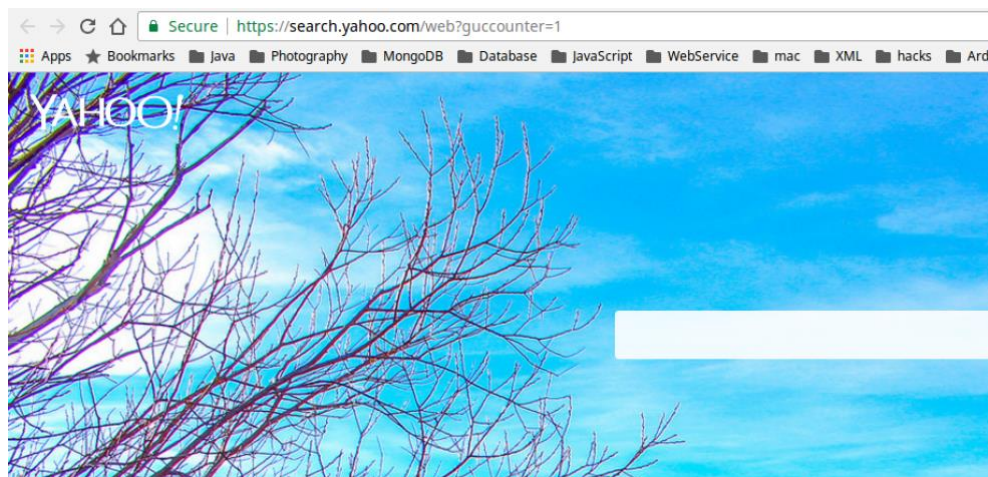
for idx, item in enumerate(sniff_search_pkts):
    if idx in indexes:
        pkt_tem = str(pkt.getlayer(Raw).fields.get("load"));
        qry = pkt_tem.split("?p=")[1].split("&")[0];
        print qry;
```

```
GET /beacon/tpc.gif?1385107348163 HTTP/1.1
Host: search.yahoo.com
Connection: keep-alive
Accept: image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Referer: http://www.yahoo.com/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: B=fmelok594jgu26b=46d=9My3dglpYEKiuRrXoAZSeDlKr2E-6s=8r6i=5J7ecf8eDYjFgm.CEdnr; AO=0=0; YLS=v=16p=16n=1; F=a=I.qqZFgMvSp1SMQ7oNaJGIBu5DA
```

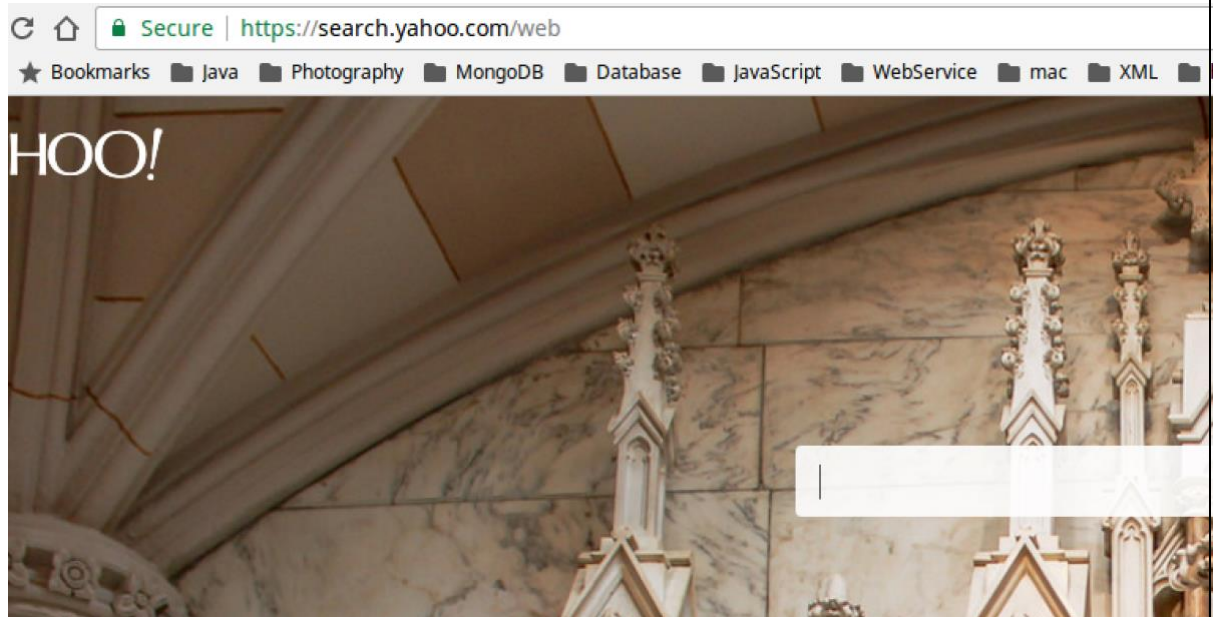
```
GET /search;_ylt=A0oG7mGbD49S8xcA3wpXNy0A;_ylc=X1MDMjc2NjY3Q0RfcgMyBGJjawNmbWVsb2s1OTRqZ3UyJTJ2YiUzRDQlMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BbWlNLRGxLcJjFLSuyNnMlMQ04ciUyNmklM0RTSjd1Y2Y4ZURZakZn
Host: search.yahoo.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Referer: http://search.yahoo.com/search;_ylt=A0oG7mGbD49S8xcA3wpXNy0A;_ylc=X1MDMjc2NjY3Q0RfcgMyBGJjawNmbWVsb2s1OTRqZ3UyJTJ2YiUzRDQlMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BbWlNLRGxLcJjFLSuyNnMlMQ04ciUyNmklM0RTSjd1Y2Y4ZURZakZn
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: B=fmelok594jgu26b=46d=9My3dglpYEKiuRrXoAZSeDlKr2E-6s=8r6i=5J7ecf8eDYjFgm.CEdnr; AO=0=0; YLS=v=16p=16n=1; F=a=I.qqZFgMvSp1SMQ7oNaJGIBu5DAJG0Z5SeRkXSkxg6_KZLWHQMHEkeFQrE0xAH9B0vMhV
00012000006r=s26lge=US6intl=us; PH=fn=y6cDg_45mcvg7WkKv--6l=en-US6i=us; T=z=0N/aSB0hmfSB1LhKlNl0DnkPNjE3NAY2Tzc2HzM3NE80TjU1Tz6a=QAE6sk=DAAF.nnTb.zm2Z&ks=EAAyagoFccuicuyK3SHedyyv...
```



```
GET /search;_ylt=A0oG7mGbD49S8xcA3wpXNy0A;_ylc=X1MDMjc2NjY3Q0RfcgMyBGJjawNmbWVsb2s1OTRqZ3UyJTJ2YiUzRDQlMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BbWlNLRGxLcJjFLSuyNnMlMQ04ciUyNmklM0RTSjd1Y2Y4ZURZakZn
Host: search.yahoo.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Referer: http://search.yahoo.com/search;_ylt=A0oG7mGbD49S8xcA3wpXNy0A;_ylc=X1MDMjc2NjY3Q0RfcgMyBGJjawNmbWVsb2s1OTRqZ3UyJTJ2YiUzRDQlMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BbWlNLRGxLcJjFLSuyNnMlMQ04ciUyNmklM0RTSjd1Y2Y4ZURZakZn
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: B=fmelok594jgu26b=46d=9My3dglpYEKiuRrXoAZSeDlKr2E-6s=8r6i=5J7ecf8eDYjFgm.CEdnr; AO=0=0; YLS=v=16p=16n=1; F=a=I.qqZFgMvSp1SMQ7oNaJGIBu5DAJG0Z5SeRkXSkxg6_KZLWHQMHEkeFQrE0xAH9B0vMhV
```



```
GET /search_ylt=A0oG7mGkD49SbxcAgG1XNy0A_ylc=X1MDMjc2NjY3OQRfcgMyBGJawNmbWVsb2s1OTRqZ3UyJTl2YlUzRDQIMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BWLlRcLcjlJFLSjYhMlM0Q4ciUyImk1MORTSjd1Y2Y4ZURZakZnbSSORWRFu
Host: search.yahoo.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Referer: http://search.yahoo.com/search_ylt=A0oG7mGkD49SbxcAgG1XNy0A_ylc=X1MDMjc2NjY3OQRfcgMyBGJawNmbWVsb2s1OTRqZ3UyJTl2YlUzRDQIMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BWLlRcLcjlJFLSjYhMlM0Q4ciUyImk1MORTSjd1Y2Y4ZURZakZnbSSORWRFu
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: B=fne1ok594jgu26b=46d=9My3dglpYEKiuRrxoAZSeDlKr2E-6s=8r6i-SJ7ecf8eDyJFgm.CEdnr; AO=0=0; YLS=v=16p=16n=1; F=a=I.qqZFgMvSp1SMQ7oNaJGIBu5DAJG025SeRxXSKxg6_KZLWHQMHEkFQRE0xAH9B0vMhwks-6b=hBj
```



```
GET /search_ylt=A0oG7mG0D49Sk08Am.NXNy0A?ei=UTF-8&fr=yfp-t-1406p=blue+bottle+coffee&spellState=sfr2=sp-qrw-corr-top HTTP/1.1
Host: search.yahoo.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Referer: http://search.yahoo.com/search_ylt=A0oG7mGkD49SbxcAgG1XNy0A_ylc=X1MDMjc2NjY3OQRfcgMyBGJawNmbWVsb2s1OTRqZ3UyJTl2YlUzRDQIMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BWLlRcLcjlJFLSjYhMlM0Q4ciUyImk1MORTSjd1Y2Y4ZURZakZnbSSORWRFu
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: B=fne1ok594jgu26b=46d=9My3dglpYEKiuRrxoAZSeDlKr2E-6s=8r6i-SJ7ecf8eDyJFgm.CEdnr; AO=0=0; YLS=v=16p=16n=1; F=a=I.qqZFgMvSp1SMQ7oNaJGIBu5DAJG025SeRxXSKxg6_KZLWHQMHEkFQRE0xAH9B0vMhwks-6b=hBj
```

Secure | https://search.yahoo.com/search_ylt=A0oG7mGkD49SbxcAgG1XNy0A_ylc=X1MDMjc2NjY3OQRfcgMyBGJawNmbWVsb2s1OTRqZ3UyJTl2YlUzRDQIMjZkJTNEOU1SM2RnMXBZRUtpdVJyeG9BWLlRcLcjlJFLSjYhMlM0Q4ciUyImk1MORTSjd1Y2Y4ZURZakZnbSSORWRFu

Bookmarks Java Photography MongoDB Database JavaScript WebService mac XML hacks Arduino Cambio Tutorials MyWorks MIS

discover? Make Yahoo Your Home Page. See breaking news & more every time you open your browser.

Blue Bottle Coffee

Web Images Video News More Anytime

Also try: [blue bottle coffee locations](#), [blue bottle coffee san francisco](#)

Ads related to: Blue Bottle coffee

Voted #1 Coffee Subscription - Premium Single Origin Coffee
[www.moustachecoffeeclub.com](#)
We learn your preferences and pick the best **coffees** just for you. From \$13
Birthday Gifts - World's Best - Delivered Fresh - Exceptionally Smooth
At the Moustache Coffee Club we roast to order and ship the same ...
Join Free Trial Gift

Specialty & Gourmet Coffee - Free Shipping with 4+ Bags
[www.volcanicacoffee.com](#)
4.5 ★★★★★ rating for volcanicacoffee.com
Volcanica Gourmet **Coffee** Beans are backed with our 100% satisfaction guarantee.
Tunac Estate, Dorset Fair Trade, Organic, Dark Roast, Gifts

Blue Bottle Coffee
Coffee roaster and retailer headquartered in Oakland, California

[bluebottlecoffee.com](#)

Blue Bottle Coffee, Inc. is a coffee roaster and retailer headquartered in Oakland, California, United States. In 2017, a majority stake in the company was acquired by Nestlé. It is considered a major player in third wave coffee. [en.wikipedia.org](#)

CEO: [W. James Freeman](#)

2. Analyze Site Visitors

- Find the IP's of site visitors

```
#!/usr/bin/env python
from scapy.all import *
from scapy.layers.inet import IP

#search_file = "search.cap";
search_file = "http.cap";
#search_file = "smtp.pcap";
packets = rdpcap(search_file);
checking_first_packet = True

client_ip_addr = None
server_ip_addr = None

temp_packets = []
messages = []

print "Find IPs from file " + search_file;
for packet in packets:
    if checking_first_packet:
        client_ip_addr = packet[IP].src
        checking_first_packet = False
    else:
        if packet[IP].src != client_ip_addr:
            server_ip_addr = packet[IP].src

    try:
        if (packet[Raw]):
            temp_packets.append(packet)
    except IndexError:
        pass

for packet in temp_packets:
    if packet[IP].src == client_ip_addr:
        messages.append({'client': str(packet[IP].src)})
    elif packet[IP].src == server_ip_addr:
        messages.append({'server': str(packet[IP].src)})

ips=[];
for msg in messages:
    if "client" in msg and msg not in ips:
        ips.append(msg)
        print msg;

Find IPs from file search.cap
{'client': '10.25.3.61'}

Process finished with exit code 0

Find IPs from file http.cap
{'client': '145.254.160.237'}

Process finished with exit code 0

Find IPs from file smtp.pcap
{'client': '10.10.1.4'}

Process finished with exit code 0
```

3. Analyze Email

- Find Email Providers,:

```
WARNING: NO ROUTE FOUND FOR IPV6 DESTINATION :: (NO DEFAULT ROUTE?)
0000 Ether / IP / UDP / DNS Qry "mail.patriots.in."
0001 Ether / IP / UDP / DNS Ans "patriots.in."
0002 Ether / IP / TCP 10.10.1.4:1470 > 74.53.140.153:smtp S
```

- Email Addresses:

```
Packet index 15 : MAIL FROM: <gurpartap@patriots.in>
Packet index 16 : 250 OK
Packet index 17 : RCPT TO: <raj_deol2002in@yahoo.co.in>
```

- Participants,

```
From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
```

- Passwords,

```
Packet index 9 : AUTH LOGIN
Packet index 10 : 334 VXNlcm5hbWU6
Packet index 11 : Z3VycGFydGFwQHBhdHJpb3RzLmlu
Packet index 12 : 334 UGFzc3dvcmQ6
Packet index 13 : cHVuamFiQDEyMw==
Packet index 14 : 235 Authentication succeeded
Packet index 15 : MAIL FROM: <gurpartap@patriots.in>
Packet index 16 : 250 OK
Packet index 17 : RCPT TO: <raj_deol2002in@yahoo.co.in>
Packet index 18 : 250 Accepted
Packet index 19 : DATA
Packet index 20 : 354 Enter message, ending with "." on a line by itself
```

- Email Client,

```
Packet index 21 : From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="-----NextPart.000.0004.01CA4580.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjJZEdeR1Kh8i+hUyVo0A==
Content-Language: en-us
x-cr-hashedpuzzle: SeA= AAR2 ADaH Bpi0 C4G1 D1gW FNB1 FPKR Fn+W HFCEP HnYJ J07s Kum6 KytW LFcI
{CAA37F59-1850-45C7-8540-AA27696B5398};ZwB1AHIAcABhAHIAAdABhAHAAQABwAGEAdABYAGkABwB0AHMALgBpAG4
x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398}
```


- Attachments,

NEWS.txt

Version 4.9.9.1

- * Many bug fixes
- * Improved editor

Version 4.9.9.0

- * Support for latest Mingw compiler system builds
- * Bug fixes

Version 4.9.8.9

- * New code tooltip display
- * Improved Indent/Unindent and Remove Comment
- * Improved automatic indent
- * Added support for the "interface" keyword
- * WebUpdate should now report installation problems from PackMan
- * New splash screen and association icons
- * Improved installer
- * Many bug fixes

Version 4.9.8.7

- * Added support for GCC > 3.2
- * Debug variables are now resent during next debug session
- * Watched Variables not in correct context are now kept and updated when = it is needed
- * Added new compiler/linker options:=20
 - Strip executable
 - Generate instructions for a specific machine (i386, i486, i586, = i686, pentium, pentium-mmx, pentiumpro, pentium2, pentium3, pentium4
- Packet index 34 : ,=20
 - k6, k6-2, k6-3, athlon, athlon-tbird, athlon-4, athlon-xp, = athlon-mp, winchip-c6, winchip2, k8, c3 and c3-2)
 - Enable use of processor specific built-in functions (mmmx, sse, = sse2, pni, 3dnow)
- * "Default" button in Compiler Options is back
- * Error messages parsing improved
- * Bug fixes

Version 4.9.8.5

- * Added the possibility to modify the value of a variable during = debugging (right click on a watch variable and select "Modify value")
- * During Dev-C++ First Time COnfiguration window, users can now choose = between using or not class browser and code completion features.
- * Many bug fixes

Version 4.9.8.4

- * Added the possibility to specify an include directory for the code = completion cache to be created at Dev-C++ first startup
- * Improved code completion cache
- * WebUpdate will now backup downloaded DevPaks in Dev-C++\Packages = directory, and Dev-C++ executable in devcpp.exe.BACKUP
- * Big speed up in function parameters listing while editing
- * Bug fixes

Version 4.9.8.3

- * On Dev-C++ first time configuration dialog, a code completion cache of =
all the standard=20
include files can now be generated.
- * Improved WebUpdate module
- * Many bug fixes

Version 4.9.8.2

- * New debug feature for DLLs: attach to a running process
- * New project option: Use custom Makefile.=20
- * New WebUpdater module.
- * Allow user to specify an alternate configuration file in Environment =
Options=20
(sti
Packet index 35 : ll can be overridden by using "-c" command line parameter).
- * Lots of bug fixes.

Version 4.9.8.1

- * When creating a DLL, the created static lib respects now the =
project-defined output directory

Version 4.9.8.0

- * Changed position of compiler/linker parameters in Project Options.
- * Improved help file
- * Bug fixes

Version 4.9.7.9

- * Resource errors are now reported in the Resource sheet
- * Many bug fixes

Version 4.9.7.8

- * Made whole bottom report control floating instead of only debug =
output.
- * Many bug fixes

Version 4.9.7.7

- * Printing settings are now saved
- * New environment options : "watch variable under mouse" and "Report =
watch errors"
- * Bug fixes

Version 4.9.7.6

- * Debug variable browser
- * Added possibility to include in a Template the Project's directories =
(include, libs and ressources)
- * Changed tint of Class browser pictures colors to match the New Look =
style
- * Bug fixes

Version 4.9.7.5

- * Bug fixes

Version 4.9.7.4

- * When compiling with debugging symbols, an extra definition is passed =
to the
compiler: -D__DEBUG__
- * Each project creates a <project_name>_private.h file containing =

version

information definitions

- * When compiling the current file only, no dependency checks are performed
- * ~300% Speed-up in class parser
- * Added "External programs" in Tools/Environment Options (for units = "Open with")
- * Added "Open with" in project units context menu
- * Added
- Packet index 37 : "Classes" toolbar
- * Fixed pre-compilation dependency checks to work correctly
- * Added new file menu entry: Save Project As
- * Bug-fix for double quotes in devcpp.cfg file read by vUpdate
- * Other bug fixes

Version 4.9.7.3

- * When adding debugging symbols on request, remove "-s" option from = linker
- * Compiling progress window
- * Environment options : "Show progress window" and "Auto-close progress = window"
- * Bug fixes

Version 4.9.7.2

- * Bug fixes

Version 4.9.7.1

- * "Build priority" per-unit
- * "Include file in linking process" per-unit
- * New feature: compile current file only
- * Separated C++ compiler options from C compiler options in Makefile = (see bug report #654744)
- * Separated C++ include dirs from C include dirs in Makefile (see bug = report #654744)
- * Necessary UI changes in Project Options
- * Added display of project filename, project output and a summary of the = project files in Project Options General tab.
- * Fixed the "compiler-dirs-with-spaces" bug that crept-in in 4.9.7.0
- * Multi-select files in project-view (when "double-click to open" is = configured in Environment Settings)
- * Resource files are treated as ordinary files now
- * Updates in "Project Options/Files" code
- * MSVC import now creates the folders structure of the original VC = project
- * Bug fixes

Version 4.9.7.0

- * Allow customizing of per-unit compile command in projects
- * Added two new macros: <DATE> and <DATETIME>
- * A
- Packet index 38 : added support for macros in the "default source code" (Tools/Editor = Options/Code)
- * Separated layout info from project file. It is now kept in a different = file (the same filename as the project's but with extension ".layout"). If = you

have your project under CVS control, you 'll know why this had to =
 happen...
 * Compiler settings per-project
 * Compiler set per-project
 * Implemented new compiler settings framework
 * "Compile as C++" per-unit
 * "Include file in compilation process" per-unit
 * Project version info (creates the relevant VERSIONINFO struct in the
 =
 private
 resource)
 * Support XP Themes (creates the CommonControls 6.0 manifest file and =
 includes
 it in the private resource)
 * Added CVS "login" and "logout" commands
 * Project manager and debugging window (in Debug tab) can now be =
 trasnformed into floating windows.
 * Added "Add Library" button in Project Options
 * Bug fixes

Version 4.9.6.9

* Implemented search in help files for the word at cursor (context =
 sensitive help)
 * Implemented "compiler sets" infrastructure to switch between
 different =
 compilers easily (e.g. gcc-2.95 and gcc-3.2)
 * Added "Files" tab in CVS form to allow selection of more than one
 file =
 for
 the requested CVS action
 =20

Version 4.9.6.8

* support for DLL application hosting, for debugging and executing DLLs
 =
 under Dev-C++.
 * New class browser option: "Show inherited members"
 * Added sup
 Packet index 40 : port for the '::' member access operator in code-
 completion
 * Added *working* function arguments hint
 * Added bracket highlighting. When the caret is on a bracket, that =
 bracket and
 its counterpart are highlighted
 * Nested folders in project view

Version 4.9.6.7

* XP Theme support
 * Added CVS commands "Add" and "Remove"
 * Added configuration option for "Templates Directory" in "Environment
 =
 Options"
 * Code-completion updates
 * Bug fixes

Version 4.9.6.6

* Editor colors are initialized properly on Dev-C++ first-run
 * Added doxygen-style comments in NewClass, NewMemberFunction and =
 NewMemberVariable wizards
 * Added file's date/time stamp in File/Properties window
 * Current windows listing in Window menu
 * Bug fixes

Version 4.9.6.5

- * CVS support
- * Window list (in Window menu)
- * bug fixes

version 4.9.6.4

- * added ENTER key for opening file in project browser, DEL to delete = from the project.
- * bug fixes

version 4.9.6.3

- * Bug fixes

version 4.9.6.2

- * Bug fixes

version 4.9.6.1

- * New "Abort compilation" button
- * Bug fixes
- * Now checks for vRoach existence when sending a crash report

Version 4.9.5.5

- * New option in Editor Options: Show editor hints. User can disable the = hints

displayed in the editor when the mouse moves over a word. Since this = was the

cause of many errors (although it should be fixed by now), we are = giving the

user the option to disable this featu

Packet index 41 : re.

- * New option in Editor Options (code-completion): Use code-completion = cache.

Well, it adds caching to code-completion. Depending on the cache size,

the program may take a bit longer to start-up, but provides very fast code-completion and the user has all the commands (belonging to the = files

he added in the cache) at his fingertips. If, for example, the user = adds

"windows.h", he gets all the WinAPI! If he adds "wx/wx.h", he gets all =

of

wxWindows! You get the picture...

- * Removed "Only show classes from current file" option in class browser = settings.

It used to be a checkbox, allowing only two states (on or off), but = there is

a third relevant option now: "Project classes" so it didn't fit the = purpose...

The user can define this in the class browser's context menu under = "View mode".

- * Fixed the dreaded "Clock skew detected" compiler warning!
- * Fixed many class browser bugs, including some that had to do with = class folders.

Version 4.9.5.4

* Under NT, 2000 and XP, user application data directory will be used to =
store config files (i.e : C:\Documents and Settings\Username\Local =
Settings\Application Data)

Version 4.9.5.3

* Added ExceptionsAnalyzer. If the devcpp.map file is in the devcpp.exe =
directory
then we even get a stack trace in the bug report!
* Added new WebUpdate module (inactive temporarily).
* Added new code for code-completion caching of fi
Packet index 43 : les (disabled - work =
in progress).

Version 4.9.5.2

* Added new option in class-browser: Use colors
(available when right-clicking the class-browser
and selecting "View mode").
* Dev-C++ now traps access violation of your programs (and of itself
too =
;)

Version 4.9.5.1

* Implemented the "File/Export/Project to HTML" function.
* Added "Tip of the day" system.
* When running a source file in explorer, don't spawn new instance.
Instead open the file in an already launched Dev-C++.
* Class-parser speed-up (50% to 85% improvement timed!!!)
* Many code-completion updates. Now takes into account context,
class inheritance and visibility (shows items only from files
#included directly or indirectly)!
* Caching of result set of code-completion for speed-up.
* New option "Execution/Parameters" (and "Debug/Parameters").

Version 4.9.5.0 (5.0 beta 5):

* CPU Window (still in development)
* ToDo list
* Backtrace in debugging
* Run to cursor
* Folders in Project and Class Browser
* Send custom commands to GDB
* Makefile can now be customized.
* Modified the behaviour of the -c param :=20
-c <config file directory>
* Saving of custom syntax parameter group
* Possibility of changing compilers and tools filename.
* Many bug fixes

Version 4.9.4.1 (5.0 beta 4.1):

* back to gcc 2.95.3
* Profiling support
* new update/packages checker (vUpdate)
* Lots of bugfixes

Conclusion

Scapy is powerful tool that can be used to packet sniffing, filtering, manipulations.

***** End *****

End – Incident-05 *****