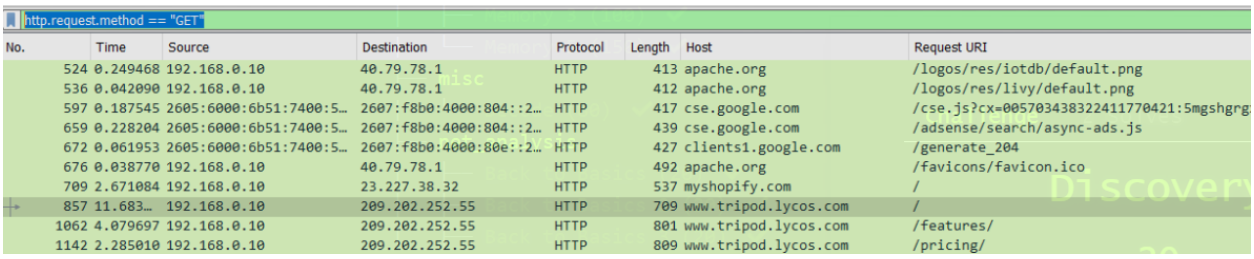
Discovery

20

In order to test basic auditing functionality, a sample of packet capture has been provided to analysts for review. Please answer the following using the provided packet capture from the server. What was the third unique webpage/domain to be requested?

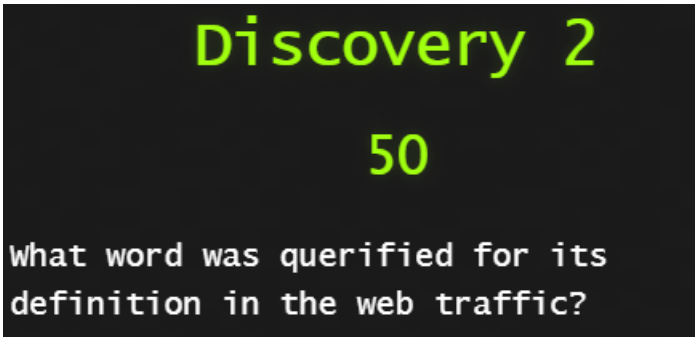
Filter: http.request.method == "GET"

Add a column for host and request uri

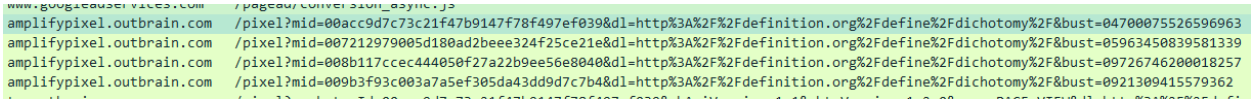


No.	Time	Source	Destination	Protocol	Length	Host	Request URI
524	0.249468	192.168.0.10	40.79.78.1	HTTP	413	apache.org	/logos/res/iotdb/default.png
536	0.042090	192.168.0.10	40.79.78.1	HTTP	412	apache.org	/logos/res/livy/default.png
597	0.187545	2605:6000:6b51:7400:5…	2607:f8b0:4000:804::2…	HTTP	417	cse.google.com	/cse.js?cx=005703438322411770421:5mgshgrg
659	0.228204	2605:6000:6b51:7400:5…	2607:f8b0:4000:804::2…	HTTP	439	cse.google.com	/adsense/search/async-ads.js
672	0.061953	2605:6000:6b51:7400:5…	2607:f8b0:4000:80e::2…	HTTP	427	clients1.google.com	/generate_204
676	0.038770	192.168.0.10	40.79.78.1	HTTP	492	apache.org	/favicons/favicon.ico
709	2.671084	192.168.0.10	23.227.38.32	HTTP	537	myshopify.com	/
857	11.683…	192.168.0.10	209.202.252.55	HTTP	709	www.tripod.lycos.com	/
1062	4.079697	192.168.0.10	209.202.252.55	HTTP	801	www.tripod.lycos.com	/features/
1142	2.285010	192.168.0.10	209.202.252.55	HTTP	809	www.tripod.lycos.com	/pricing/

Flag: tripod.lycos.com

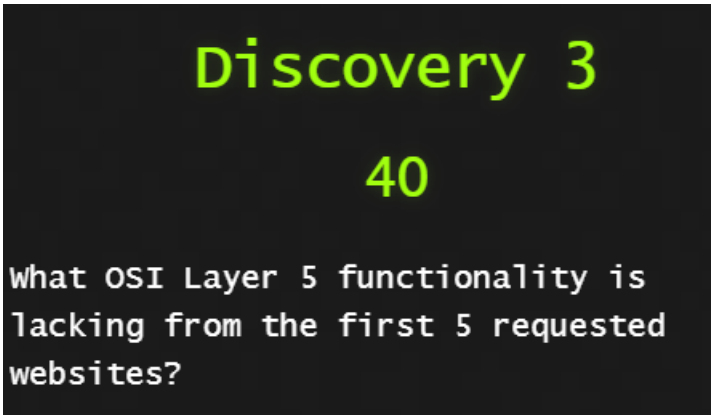


Filter: http.request.method == "GET"

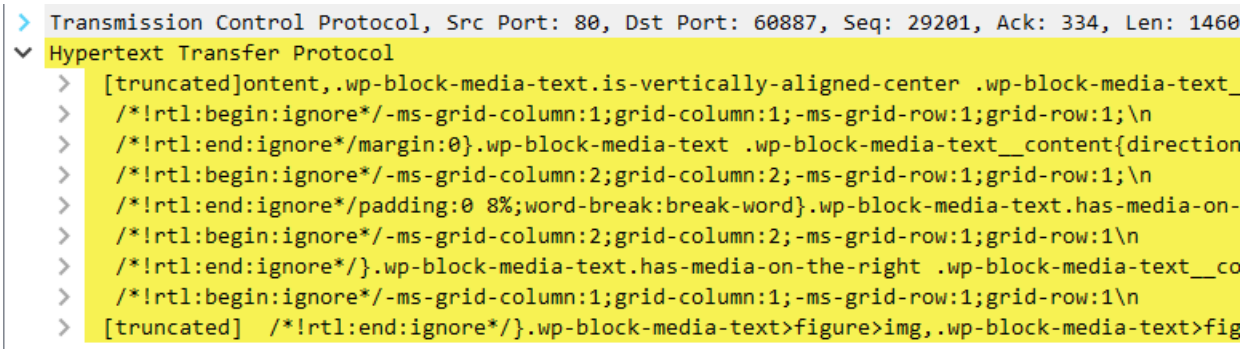


We see definition.org looking for dichotomy.

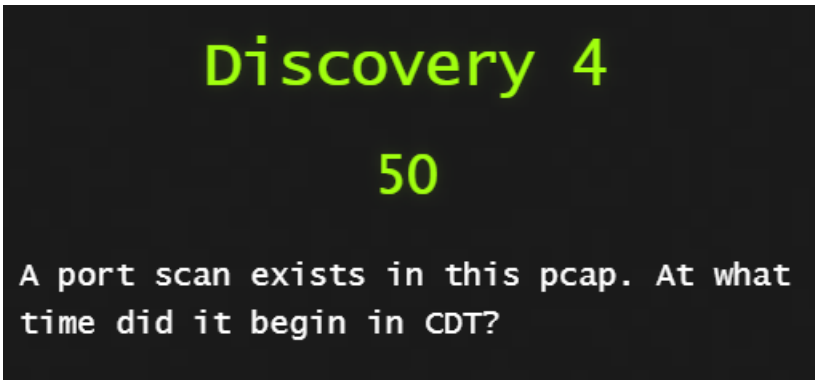
Flag: dichotomy



The first few websites are easily readable, so there is not encryption going on so there is no ssl



Flag: ssl

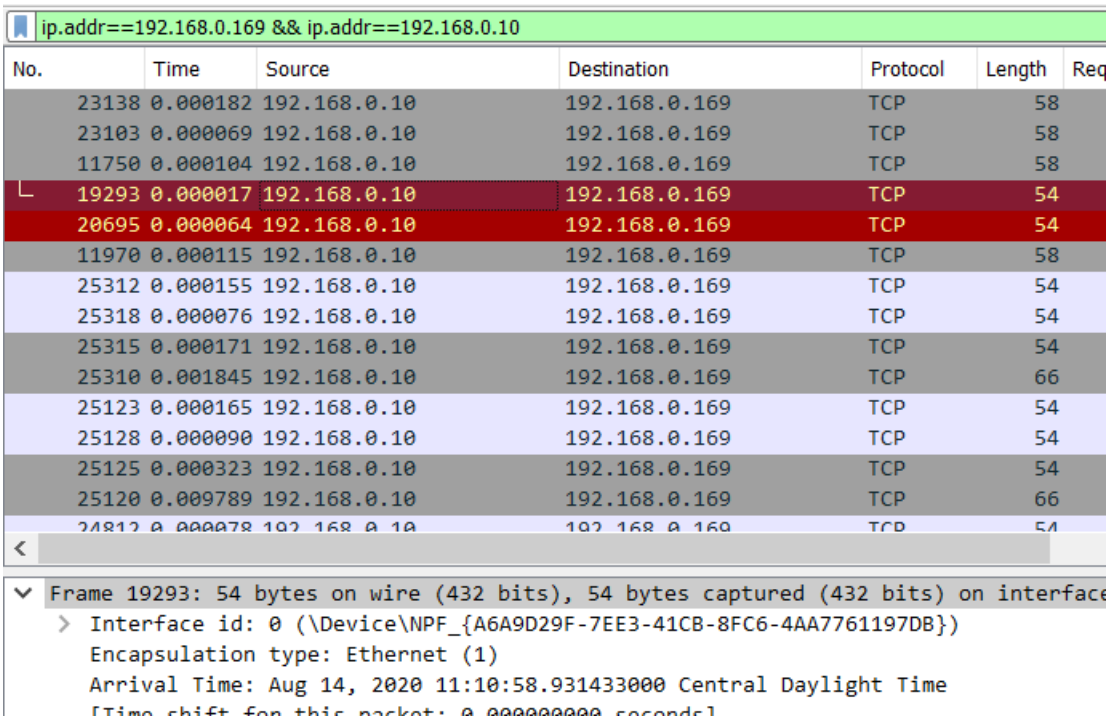


Looking at the statistics conversations we see that there is some communication from

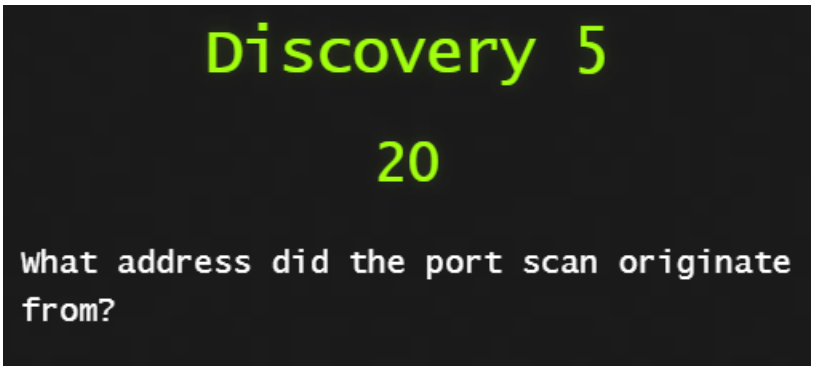
192.168.0.169	60874	192.168.0.10	14147	2	
192.168.0.169	60885	192.168.0.10	14147	2	
192.168.0.169	60874	192.168.0.10	8005	2	
192.168.0.169	60874	192.168.0.10	20	2	
192.168.0.10	60885	128.197.236.4	80	3	
192.168.0.169	60874	192.168.0.10	8080	3	
192.168.0.169	60874	192.168.0.10	3306	3	
192.168.0.169	60874	192.168.0.10	110	3	
192.168.0.169	60874	192.168.0.10	80	3	
192.168.0.169	60874	192.168.0.10	25	3	
192.168.0.169	60874	192.168.0.10	143	3	
192.168.0.169	60874	192.168.0.10	443	3	
192.168.0.169	60874	192.168.0.10	21	3	
192.168.0.169	60874	192.168.0.10	79	3	
192.168.0.169	60874	192.168.0.10	106	3	
192.168.0.169	60874	192.168.0.10	105	3	
192.168.0.169	60874	192.168.0.10	2224	3	
192.168.0.10	60884	128.197.236.4	80	6	
192.168.0.10	60401	23.227.38.32	80	7	
192.168.0.10	60678	98.139.28.144	80	7	

ip.addr==192.168.0.169 && ip.addr==192.168.0.10

It starts out at 11:10



Flag: 11:10

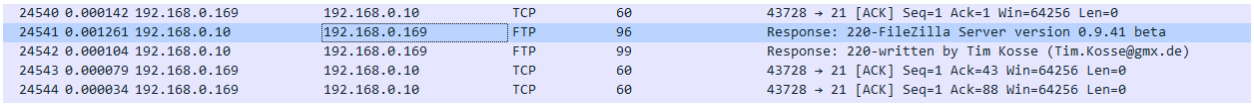


Flag: 192.168.0.169

Discovery 6

50

Which protocol did the address connect to and then use?



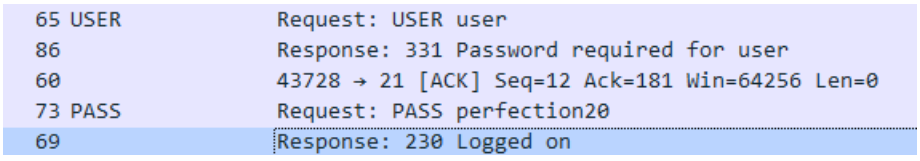
24540	0.000142	192.168.0.169	192.168.0.10	TCP	60	43728 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0
24541	0.001261	192.168.0.10	192.168.0.169	FTP	96	Response: 220-FileZilla Server version 0.9.41 beta
24542	0.000104	192.168.0.10	192.168.0.169	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
24543	0.000079	192.168.0.169	192.168.0.10	TCP	60	43728 → 21 [ACK] Seq=1 Ack=43 Win=64256 Len=0
24544	0.000034	192.168.0.169	192.168.0.10	TCP	60	43728 → 21 [ACK] Seq=1 Ack=88 Win=64256 Len=0

Flag: ftp

Discovery 7

50

Which 2 values were input to establish a connection? Answer: value1/value2



65	USER	Request: USER user
86		Response: 331 Password required for user
60		43728 → 21 [ACK] Seq=12 Ack=181 Win=64256 Len=0
73	PASS	Request: PASS perfection20
69		Response: 230 Logged on

Flag: user/perfection20


```
83                  Response: 200 Port command successful
72 RETR             Request: RETR 14aug20.txt
66                  20 → 41705 [SYN] Seq=0 Win=64240 Len=0
66                  41705 → 20 [SYN, ACK] Seq=0 Ack=1 Win=
```

Flag: 14aug20.txt

Look at the ftp-data stream of the 14aug20.txt

ftp-data

No.	Time	Source	Destination	Protocol	Length	Request command	Info
24814	0.000000	192.168.0.10	192.168.0.169	FTP-DATA	1860		FTP Data: 1806 bytes (PORT) (LIST)
24935	5.700012	192.168.0.10	192.168.0.169	FTP-DATA	711		FTP Data: 657 bytes (PORT) (LIST)
25124	4.114809	192.168.0.10	192.168.0.169	FTP-DATA	2509		FTP Data: 2455 bytes (PORT) (LIST)
25314	13.812…	192.168.0.10	192.168.0.169	FTP-DATA	117		FTP Data: 63 bytes (PORT) (RETR 14aug20.txt)

Wireshark · Follow TCP Stream (tcp.stream eq 474) · discovery.pcapng

```
10:43 AM 8/14/2020 Deposit $1000 in John Dough bonus account.
```

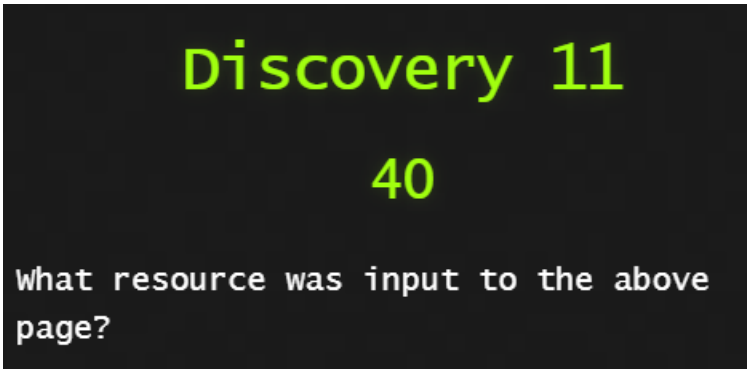
Flag: $1000

Filter: http.host ==192.168.0.10

http.host ==192.168.0.10

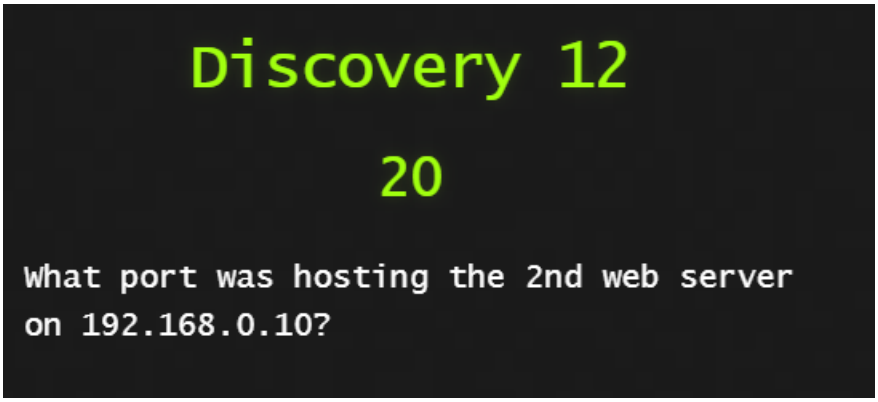
No.	Time	Source	Destination	Protocol	Length	Request command	Request Method	Info
32265	0.000000	192.168.0.169	192.168.0.10	HTTP	437		GET	GET /dvwa HTTP/1.1
32268	0.006889	192.168.0.169	192.168.0.10	HTTP	438		GET	GET /dvwa/ HTTP/1.1
32272	0.014645	192.168.0.169	192.168.0.10	HTTP	447		GET	GET /dvwa/login.php HTTP/1.1
32275	0.017150	192.168.0.169	192.168.0.10	HTTP	447		GET	GET /dvwa/setup.php HTTP/1.1
32278	0.057743	192.168.0.169	192.168.0.10	HTTP	418		GET	GET /dvwa/js/add_event_listeners.js HTTP/1.1
32285	0.022877	192.168.0.169	192.168.0.10	HTTP	418		GET	GET /dvwa/js/add_event_listeners.js HTTP/1.1
32327	3.721412	192.168.0.169	192.168.0.10	HTTP	641		POST	POST /dvwa/setup.php HTTP/1.1 (application/x-www-form-urlencoded)
32329	0.030475	192.168.0.169	192.168.0.10	HTTP	492		GET	GET /dvwa/setup.php HTTP/1.1
32332	0.041821	192.168.0.169	192.168.0.10	HTTP	418		GET	GET /dvwa/js/add_event_listeners.js HTTP/1.1
32339	0.015688	192.168.0.169	192.168.0.10	HTTP	418		GET	GET /dvwa/js/add_event_listeners.js HTTP/1.1

Flag: /dvwa




```
GET             GET /dvwa/js/add_event_listeners.js HTTP/1.1
POST            POST /dvwa/setup.php HTTP/1.1  (application/x-www-form-urlencoded)
GET             GET /dvwa/setup.php HTTP/1.1
```

Flag: setup.php



Filter: http&& ip.dst == 192.168.0.10

http&& ip.dst == 192.168.0.10

No.	Time	Source	Destination	Protocol	Length	Host	Request Method	Info
39303	0.356436	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39317	4.686489	192.168.0.169	192.168.0.10	HTTP	458	192.168.0.10:8080	GET	GET /docs/ HTTP/1.1
39323	0.054275	192.168.0.169	192.168.0.10	HTTP	401	192.168.0.10:8080	GET	GET /docs/images/tomcat.gif HTTP/1.1
39327	0.001743	192.168.0.169	192.168.0.10	HTTP	403	192.168.0.10:8080	GET	GET /docs/images/asf-logo.svg HTTP/1.1
39343	0.262508	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39366	2.514407	192.168.0.169	192.168.0.10	HTTP	465	192.168.0.10:8080	GET	GET /docs/config/ HTTP/1.1
39399	2.483358	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39437	2.291352	192.168.0.169	192.168.0.10	HTTP	467	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39518	3.016661	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39588	2.644195	192.168.0.169	192.168.0.10	HTTP	514	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39631	2.045156	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39656	3.601811	192.168.0.169	192.168.0.10	HTTP	514	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39716	1.390631	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)

Flag: 8080

Discovery 13

40

Was the status query performed on the 2nd webserver successful?

39437	2.291352	192.168.0.169	192.168.0.10	HTTP	467	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39518	3.016661	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39588	2.644195	192.168.0.169	192.168.0.10	HTTP	514	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39631	2.045156	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39656	3.601811	192.168.0.169	192.168.0.10	HTTP	514	192.168.0.10:8080	GET	GET /manager/status HTTP/1.1
39716	1.390631	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39764	5.010485	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)
39866	5.027431	13.225.48.90	192.168.0.10	HTTP	1020			HTTP/1.1 200 OK (text/html)

```
GET /manager/status HTTP/1.1
Host: 192.168.0.10:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/2
Accept: text/html,application/xhtml+xml,application/xml;q=0.
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.10:8080/
Connection: keep-alive
Cookie: PHPSESSID=39kd258jl3h6rb3drq5uih4jjd
Upgrade-Insecure-Requests: 1
Authorization: Basic dXNlcjpwZXJmZWN0aW9uMTk=

HTTP/1.1 401 Unauthorized
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 GMT
WWW-Authenticate: Basic realm="Tomcat Manager Application"
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2562
Date: Fri, 14 Aug 2020 16:14:04 GMT
```

Flag: No