

# Network Forensics Analysis

A. Either, from NetworkSims.com ProfSIMS, select **Toolkit** from **Test Center**.

or, download:

<http://buchananweb.co.uk/dotnetclientserver.zip>

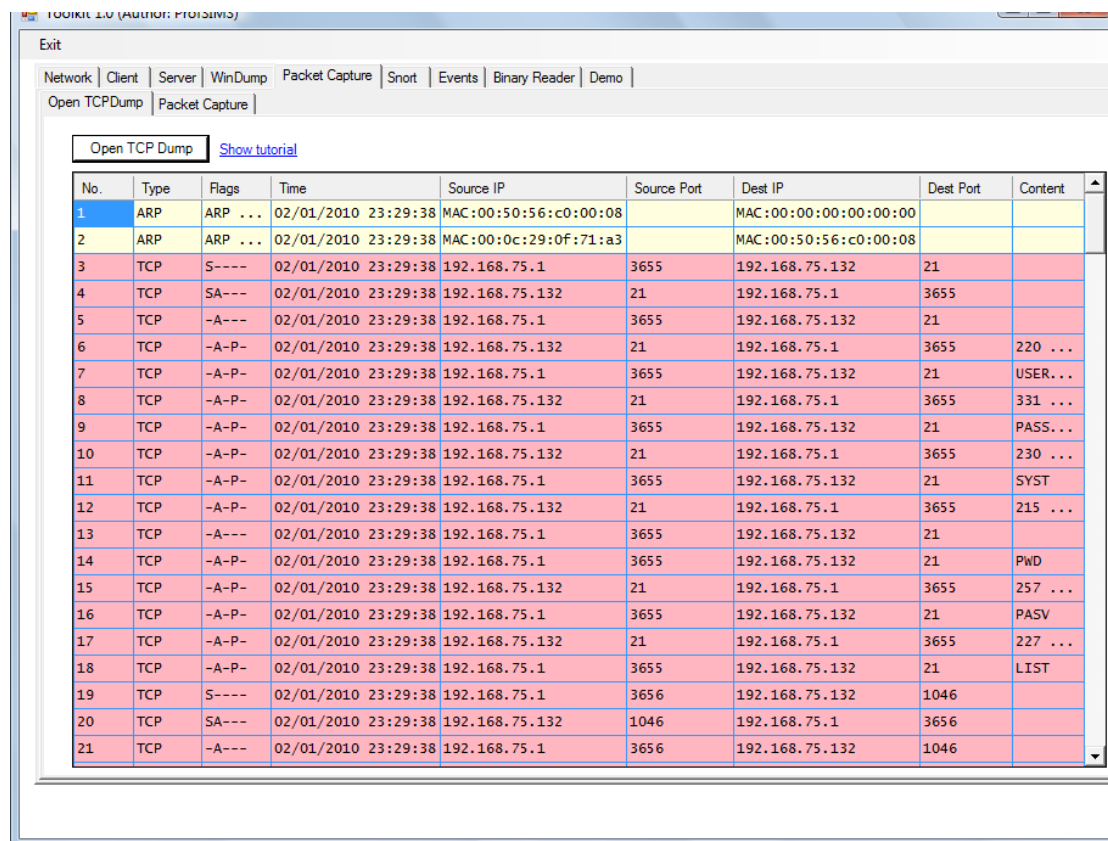
and extract to a local folder, and run client.exe.

B. Within Toolkit, select the Packet Capture tab and then the Open TCPDump tab.

## FTP Analysis Demo:

[http://buchananweb.co.uk/adv\\_security\\_and\\_network\\_forensics/tcpdump01/tcpdump01.htm](http://buchananweb.co.uk/adv_security_and_network_forensics/tcpdump01/tcpdump01.htm)

### 1.1 Open ftp dump (see Figure 1.1).



No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	ARP	ARP ...	02/01/2010 23:29:38	MAC:00:50:56:c0:00:08		MAC:00:00:00:00:00:00		
2	ARP	ARP ...	02/01/2010 23:29:38	MAC:00:0c:29:0f:71:a3		MAC:00:50:56:c0:00:08		
3	TCP	S----	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	
4	TCP	SA---	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	
5	TCP	-A---	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	
6	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	220 ...
7	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	USER ...
8	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	331 ...
9	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	PASS ...
10	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	230 ...
11	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	SYST
12	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	215 ...
13	TCP	-A---	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	
14	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	PWD
15	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	257 ...
16	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	PASV
17	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.132	21	192.168.75.1	3655	227 ...
18	TCP	-A-P-	02/01/2010 23:29:38	192.168.75.1	3655	192.168.75.132	21	LIST
19	TCP	S----	02/01/2010 23:29:38	192.168.75.1	3656	192.168.75.132	1046	
20	TCP	SA---	02/01/2010 23:29:38	192.168.75.132	1046	192.168.75.1	3656	
21	TCP	-A---	02/01/2010 23:29:38	192.168.75.1	3656	192.168.75.132	1046	

Figure 1.1: FTP Dump

Determine the following:

**Host src TCP port (Hint: Examine the Source Port on Packet 3):**

**3655**

**Server src TCP port (Hint: Examine the Destination Port on Packet 3):**

**Host src IP address (Hint: Examine the Source IP on Packet 3):**

**Server src IP address (Hint: Examine the Dest IP on Packet 3):**

**What is the MAC address of the server (Hint: Examine the reply for Packet 2):**

**Identify the packets used for the SYN, SYN/ACK and ACK sequence (Hint: packets 3 to 5 look interesting):**

**Which is the return code used by the FTP server to identify:**

**Password Required (Hint: Examine the content on Packet 9):**

**Server type (Hint: Examine the content on Packet 12):**

**Which FTP command is used to determine the current working folder (Hint: Examine the content on Packet 15):**

**Which FTP command is used to determine the files in a folder (Hint: Examine the content on Packet 18):**

**Which FTP port has been used for the FTP directory list (hint: Examine the contents of Packet 17, and the last two digits of the 227 response (first multiplied by 256 added to the second):**

**Identify the data packets used to list the contents (Hint port 1046 looks interesting):**

**Which FTP port has been used for the FTP file transfer (hint: it is the last two digits of the 227 response (first multiplied by 256 added to the second):**

**Identify the data packets used to transfer the file:**

**What is the name of the file transferred:**

1.2 Open Telnet dump (see Figure 1.2).

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	TCP	S----	02/01/2010 23:32:12	192.168.75.1	3714	192.168.75.132	23	
2	TCP	SA---	02/01/2010 23:32:12	192.168.75.132	23	192.168.75.1	3714	
3	TCP	-A---	02/01/2010 23:32:12	192.168.75.1	3714	192.168.75.132	23	
4	ARP	ARP ...	02/01/2010 23:32:17	MAC:00:0c:29:0f:71:a3		MAC:00:00:00:00:00:00		
5	ARP	ARP ...	02/01/2010 23:32:17	MAC:00:50:56:f5:2e:f3		MAC:00:0c:29:0f:71:a3		
6	UDP		02/01/2010 23:32:17	192.168.75.132	1034	192.168.75.2	53	~B~...
7	UDP		02/01/2010 23:32:18	192.168.75.2	53	192.168.75.132	1034	~B??...
8	UDP		02/01/2010 23:32:18	192.168.75.132	137	192.168.75.1	137	?3~...
9	UDP		02/01/2010 23:32:18	192.168.75.1	137	192.168.75.132	137	?3?~...
10	TCP	-A-P-	02/01/2010 23:32:18	192.168.75.132	23	192.168.75.1	3714	??%?...
11	TCP	-A-P-	02/01/2010 23:32:18	192.168.75.1	3714	192.168.75.132	23	??%
12	TCP	-A-P-	02/01/2010 23:32:18	192.168.75.132	23	192.168.75.1	3714	??%~...
13	TCP	-A-P-	02/01/2010 23:32:18	192.168.75.1	3714	192.168.75.132	23	??~?...
14	TCP	-A-P-	02/01/2010 23:32:18	192.168.75.132	23	192.168.75.1	3714	??'~...
15	TCP	-A---	02/01/2010 23:32:18	192.168.75.1	3714	192.168.75.132	23	
16	TCP	-A-P-	02/01/2010 23:32:20	192.168.75.1	3714	192.168.75.132	23	??%~...
17	TCP	-A-P-	02/01/2010 23:32:20	192.168.75.132	23	192.168.75.1	3714	??%~...
18	TCP	-A-P-	02/01/2010 23:32:20	192.168.75.1	3714	192.168.75.132	23	??'~...
19	TCP	-A---	02/01/2010 23:32:20	192.168.75.132	23	192.168.75.1	3714	
20	TCP	-A-P-	02/01/2010 23:32:20	192.168.75.1	3714	192.168.75.132	23	??%~...
21	TCP	-A-P-	02/01/2010 23:32:20	192.168.75.132	23	192.168.75.1	3714	??%~...

Figure 1.2: Telnet dump

Determine the following:

**Host src TCP port:**

**Server src TCP port:**

**Host src IP address:**

**Server src IP address:**

**Identify the packets used for the SYN, SYN/ACK and ACK sequence:**

Which is the return code used by the FTP server to identify:

**Password Required:**

**Server type:**

**Which FTP command is used to determine the current working folder:**

**Which FTP command is used to determine the files in a folder:**

**Which FTP port has been used for the FTP directory list (hint: it is the last two digits of the 227 response (first multiplied by 256 added to the second):**

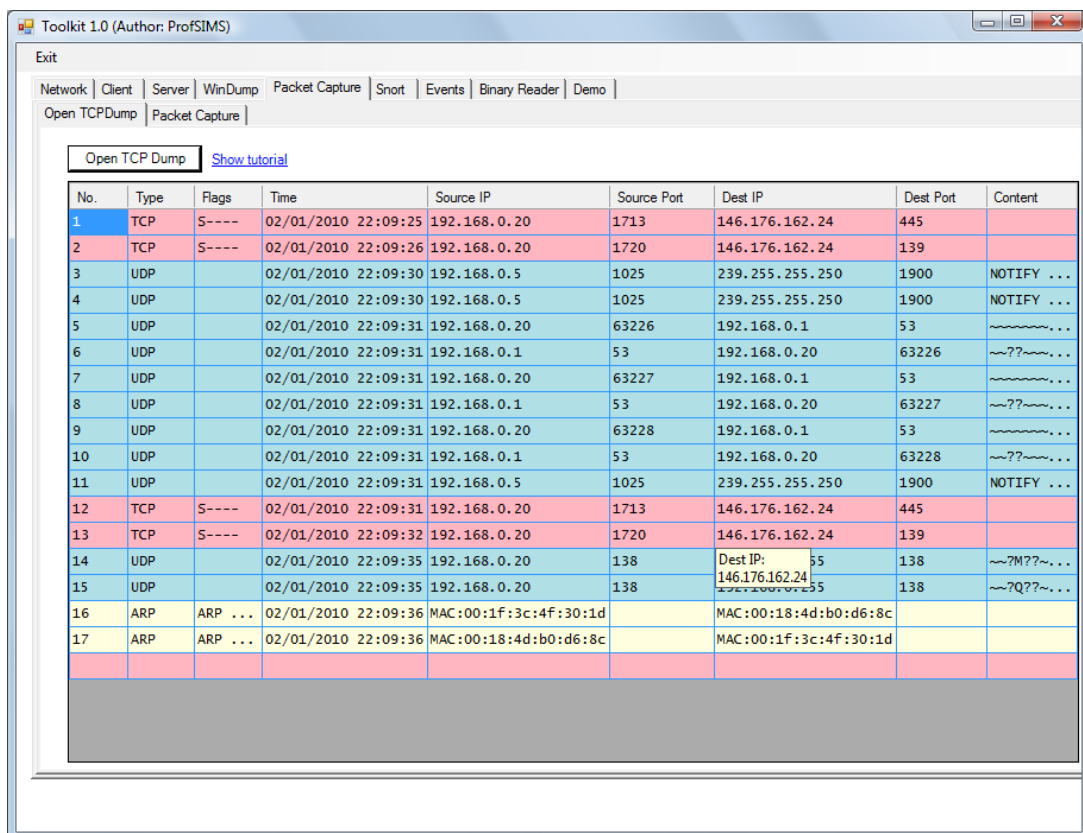
Identify the data packets used to list the contents:

Which FTP port has been used for the FTP file transfer (hint: it is the last two digits of the 227 response (first multiplied by 256 added to the second):

Identify the data packets used to transfer the file:

What is the name of the file transferred:

### 1.3 Open dns dump (see Figure 1.3).



The screenshot shows a network dump window titled 'Toolkit 1.0 (Author: ProfSIMS)'. The window contains a menu bar with options: Exit, Network, Client, Server, WinDump, Packet Capture, Snort, Events, Binary Reader, Demo. Below the menu bar, there are buttons for 'Open TCPDump' and 'Packet Capture'. A table displays the network dump data with columns: No., Type, Flags, Time, Source IP, Source Port, Dest IP, Dest Port, and Content. The table contains 17 rows of data, including TCP, UDP, and ARP packets.

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	TCP	S----	02/01/2010 22:09:25	192.168.0.20	1713	146.176.162.24	445	
2	TCP	S----	02/01/2010 22:09:26	192.168.0.20	1720	146.176.162.24	139	
3	UDP		02/01/2010 22:09:30	192.168.0.5	1025	239.255.255.250	1900	NOTIFY ...
4	UDP		02/01/2010 22:09:30	192.168.0.5	1025	239.255.255.250	1900	NOTIFY ...
5	UDP		02/01/2010 22:09:31	192.168.0.20	63226	192.168.0.1	53	~~~~~...
6	UDP		02/01/2010 22:09:31	192.168.0.1	53	192.168.0.20	63226	??~...
7	UDP		02/01/2010 22:09:31	192.168.0.20	63227	192.168.0.1	53	??~...
8	UDP		02/01/2010 22:09:31	192.168.0.1	53	192.168.0.20	63227	??~...
9	UDP		02/01/2010 22:09:31	192.168.0.20	63228	192.168.0.1	53	~~~~~...
10	UDP		02/01/2010 22:09:31	192.168.0.1	53	192.168.0.20	63228	??~...
11	UDP		02/01/2010 22:09:31	192.168.0.5	1025	239.255.255.250	1900	NOTIFY ...
12	TCP	S----	02/01/2010 22:09:31	192.168.0.20	1713	146.176.162.24	445	
13	TCP	S----	02/01/2010 22:09:32	192.168.0.20	1720	146.176.162.24	139	
14	UDP		02/01/2010 22:09:35	192.168.0.20	138	Dest IP: 146.176.162.24	138	??M??...
15	UDP		02/01/2010 22:09:35	192.168.0.20	138	146.176.162.24	138	??Q??...
16	ARP	ARP ...	02/01/2010 22:09:36	MAC:00:1f:3c:4f:30:1d		MAC:00:18:4d:b0:d6:8c		
17	ARP	ARP ...	02/01/2010 22:09:36	MAC:00:18:4d:b0:d6:8c		MAC:00:1f:3c:4f:30:1d		

Figure 1.3: DNS dump

Determine the following:

What is the transport layer used for DNS:

Host src UDP port:

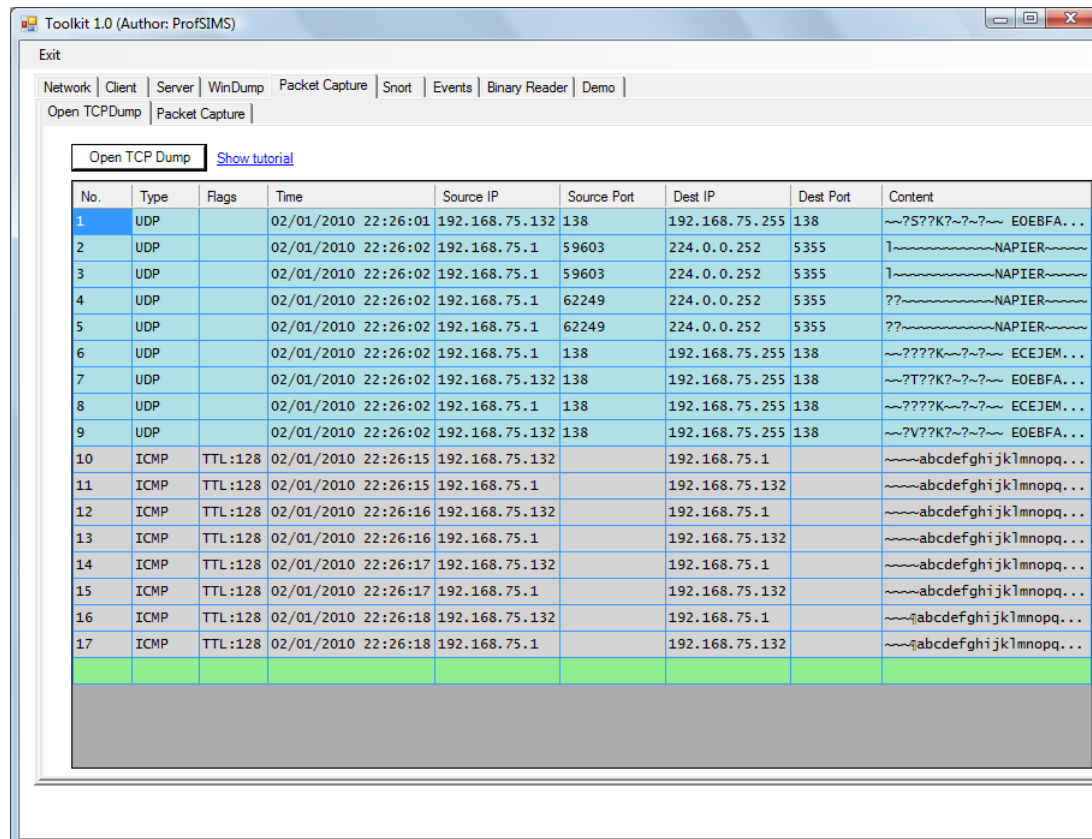
Server (DNS) src UDP port:

Host src IP address:

**Server (DNS) src IP address:**

**Identify the data packets used to for the DNS lookup:**

#### 1.4 Open ping dump (see Figure 1.4).



No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	UDP		02/01/2010 22:26:01	192.168.75.132	138	192.168.75.255	138	~?S??K?~?~ EOE BFA...
2	UDP		02/01/2010 22:26:02	192.168.75.1	59603	224.0.0.252	5355	1~NAPIER~
3	UDP		02/01/2010 22:26:02	192.168.75.1	59603	224.0.0.252	5355	1~NAPIER~
4	UDP		02/01/2010 22:26:02	192.168.75.1	62249	224.0.0.252	5355	??~NAPIER~
5	UDP		02/01/2010 22:26:02	192.168.75.1	62249	224.0.0.252	5355	??~NAPIER~
6	UDP		02/01/2010 22:26:02	192.168.75.1	138	192.168.75.255	138	~???K~?~ ECEJEM...
7	UDP		02/01/2010 22:26:02	192.168.75.132	138	192.168.75.255	138	~T??K?~?~ EOE BFA...
8	UDP		02/01/2010 22:26:02	192.168.75.1	138	192.168.75.255	138	~???K~?~ ECEJEM...
9	UDP		02/01/2010 22:26:02	192.168.75.132	138	192.168.75.255	138	~?V??K?~?~ EOE BFA...
10	ICMP	TTL:128	02/01/2010 22:26:15	192.168.75.132		192.168.75.1		~abcdefghijklmnop...
11	ICMP	TTL:128	02/01/2010 22:26:15	192.168.75.1		192.168.75.132		~abcdefghijklmnop...
12	ICMP	TTL:128	02/01/2010 22:26:16	192.168.75.132		192.168.75.1		~abcdefghijklmnop...
13	ICMP	TTL:128	02/01/2010 22:26:16	192.168.75.1		192.168.75.132		~abcdefghijklmnop...
14	ICMP	TTL:128	02/01/2010 22:26:17	192.168.75.132		192.168.75.1		~abcdefghijklmnop...
15	ICMP	TTL:128	02/01/2010 22:26:17	192.168.75.1		192.168.75.132		~abcdefghijklmnop...
16	ICMP	TTL:128	02/01/2010 22:26:18	192.168.75.132		192.168.75.1		~abcdefghijklmnop...
17	ICMP	TTL:128	02/01/2010 22:26:18	192.168.75.1		192.168.75.132		~abcdefghijklmnop...

Figure 1.4: ICMP dump

Determine the following:

**Host src IP address:**

**Server (DNS) src IP address:**

**Identify the data packets used to for the ping:**

**How many ECHO's where send from the host, and how many replies where there:**

#### 1.5 Open webpage dump (see Figure 1.5).

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	ARP	ARP ...	02/01/2010 22:33:05	MAC:00:50:56:c0:00:08		MAC:00:00:00:00:00:00		
2	ARP	ARP ...	02/01/2010 22:33:05	MAC:00:0c:29:0f:71:a3		MAC:00:50:56:c0:00:08		
3	TCP	S----	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
4	TCP	SA---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	
5	TCP	-A---	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
6	TCP	-A-P-	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	GET ...
7	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	HTTP ...
8	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	...
9	TCP	-A---	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
10	TCP	-A-P-	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	ODY>...
11	TCP	-A-P-	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	GET ...
12	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	HTTP...
13	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	rdan...
14	TCP	-A---	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
15	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	ND-C...
16	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	16p...
17	TCP	-A---	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
18	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	ATIO...
19	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	IZE:...
20	TCP	-A---	02/01/2010 22:33:05	192.168.75.1	2427	192.168.75.132	80	
21	TCP	-A---	02/01/2010 22:33:05	192.168.75.132	80	192.168.75.1	2427	-FAM...

Figure 1.5: Web dump

Determine the following:

**Host src TCP port:**

**Server src TCP port:**

**Host src IP address:**

**Server src IP address:**

**Identify the packets used for the SYN, SYN/ACK and ACK sequence:**

**What is the HTTP command used to get the default page (Hint: put your cursor over the content of the 4<sup>th</sup> data packet):**

**What is the HTTP response to a successful request (Hint: put your cursor over the content of the 5<sup>th</sup> data packet):**

1.6 Open **hping\_fin** dump (see Figure 1.6). We can see that a remote host is sending TCP segments with the FIN flag sent.

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	TCP	--F--	04/01/2010 10:34:49	192.168.75.137	1118	192.168.75.1	0	eth0
2	TCP	--F--	04/01/2010 10:34:50	192.168.75.137	1119	192.168.75.1	0	eth0
3	TCP	--F--	04/01/2010 10:34:51	192.168.75.137	1120	192.168.75.1	0	eth0
4	TCP	--F--	04/01/2010 10:34:52	192.168.75.137	1121	192.168.75.1	0	eth0
5	TCP	--F--	04/01/2010 10:34:53	192.168.75.137	1122	192.168.75.1	0	eth0
6	ARP	ARP ...	04/01/2010 10:34:54	MAC:00:0c:29:6b:0e:96		MAC:00:00:00:00:00:00		
7	ARP	ARP ...	04/01/2010 10:34:54	MAC:00:50:56:c0:00:08		MAC:00:0c:29:6b:0e:96		
8	TCP	--F--	04/01/2010 10:34:54	192.168.75.137	1123	192.168.75.1	0	eth0
9	TCP	--F--	04/01/2010 10:34:55	192.168.75.137	1124	192.168.75.1	0	eth0
10	TCP	--F--	04/01/2010 10:34:56	192.168.75.137	1125	192.168.75.1	0	eth0
11	TCP	--F--	04/01/2010 10:34:57	192.168.75.137	1126	192.168.75.1	0	eth0
12	TCP	--F--	04/01/2010 10:34:58	192.168.75.137	1127	192.168.75.1	0	eth0
13	TCP	--F--	04/01/2010 10:34:59	192.168.75.137	1128	192.168.75.1	0	eth0
14	TCP	--F--	04/01/2010 10:35:00	192.168.75.137	1129	192.168.75.1	0	eth0
15	TCP	--F--	04/01/2010 10:35:01	192.168.75.137	1130	192.168.75.1	0	eth0

Figure 1.6: hping\_fin dump

Determine the following:

**Sending src TCP port range:**

**Receiver src TCP port:**

**Sending src IP address:**

**Receiver src IP address:**

- 1.7 Open **hping\_port80** dump (see Figure 1.7). We can see that a remote host is sending TCP segments with the SYN flag sent.

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	UDP		04/01/2010 10:30:59	192.168.75.1	138	192.168.75.255	138	~??. . .
2	TCP	S----	04/01/2010 10:31:03	192.168.75.137	1608	192.168.75.1	80	eth0
3	TCP	S----	04/01/2010 10:31:04	192.168.75.137	1609	192.168.75.1	80	eth0
4	TCP	S----	04/01/2010 10:31:05	192.168.75.137	1610	192.168.75.1	80	eth0
5	TCP	S----	04/01/2010 10:31:06	192.168.75.137	1611	192.168.75.1	80	eth0
6	TCP	S----	04/01/2010 10:31:07	192.168.75.137	1612	192.168.75.1	80	eth0
7	ARP	ARP ...	04/01/2010 10:31:08	MAC:00:0c:29:6b:0e:96		MAC:00:00:00:00:00:00		
8	ARP	ARP ...	04/01/2010 10:31:08	MAC:00:50:56:c0:00:08		MAC:00:0c:29:6b:0e:96		
9	TCP	S----	04/01/2010 10:31:08	192.168.75.137	1613	192.168.75.1	80	eth0
10	TCP	S----	04/01/2010 10:31:09	192.168.75.137	1614	192.168.75.1	80	eth0
11	TCP	S----	04/01/2010 10:31:10	192.168.75.137	1615	192.168.75.1	80	eth0
12	TCP	S----	04/01/2010 10:31:11	192.168.75.137	1616	192.168.75.1	80	eth0
13	TCP	S----	04/01/2010 10:31:12	192.168.75.137	1617	192.168.75.1	80	eth0
14	TCP	S----	04/01/2010 10:31:13	192.168.75.137	1618	192.168.75.1	80	eth0
15	TCP	S----	04/01/2010 10:31:14	192.168.75.137	1619	192.168.75.1	80	eth0
16	TCP	S----	04/01/2010 10:31:15	192.168.75.137	1620	192.168.75.1	80	eth0
17	TCP	S----	04/01/2010 10:31:16	192.168.75.137	1621	192.168.75.1	80	eth0
18	TCP	S----	04/01/2010 10:31:17	192.168.75.137	1622	192.168.75.1	80	eth0
19	TCP	S----	04/01/2010 10:31:18	192.168.75.137	1623	192.168.75.1	80	eth0
20	TCP	S----	04/01/2010 10:31:19	192.168.75.137	1624	192.168.75.1	80	eth0
21	TCP	S----	04/01/2010 10:31:20	192.168.75.137	1625	192.168.75.1	80	eth0

Figure 1.7: hping\_fin dump

Determine the following:

**Sending src TCP port range:**

**Receiver src TCP port:**

**Sending src IP address:**

**Receiver src IP address:**

1.8 Open **hydra\_ftp** dump (see Figure 1.8). We can see that a Hydra attack has been conducted on our server.

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18157	192.168.75.132	21	
2	TCP	SA---	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18157	
3	TCP	-A---	04/01/2010 10:19:34	192.168.75.1	18157	192.168.75.132	21	
4	TCP	-A-P-	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18157	220 Microsoft FTP ...
5	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18158	192.168.75.132	21	
6	TCP	SA---	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18158	
7	TCP	-A---	04/01/2010 10:19:34	192.168.75.1	18158	192.168.75.132	21	
8	TCP	-A-P-	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18158	220 Microsoft FTP ...
9	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18159	192.168.75.132	21	
10	TCP	SA---	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18159	
11	TCP	-A---	04/01/2010 10:19:34	192.168.75.1	18159	192.168.75.132	21	
12	TCP	-A-P-	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18159	220 Microsoft FTP ...
13	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18160	192.168.75.132	21	
14	TCP	SA---	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18160	
15	TCP	-A---	04/01/2010 10:19:34	192.168.75.1	18160	192.168.75.132	21	
16	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18161	192.168.75.132	21	
17	TCP	SA---	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18161	
18	TCP	-A---	04/01/2010 10:19:34	192.168.75.1	18161	192.168.75.132	21	
19	TCP	-A-P-	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18160	220 Microsoft FTP ...
20	TCP	S----	04/01/2010 10:19:34	192.168.75.1	18162	192.168.75.132	21	
21	TCP	-A-P-	04/01/2010 10:19:34	192.168.75.132	21	192.168.75.1	18161	220 Microsoft FTP ...

Figure 1.8: Hydra\_ftp dump

Determine the following:

**Sending src TCP port range:**

**Receiver src TCP port:**

**Sending src IP address:**

**Receiver src IP address:**

**What are the logins used:**

**What are the passwords used:**

**What is the successful login/password:**

1.9 Open **hydra\_telnet** dump (see Figure 1.9). We can see that a Hydra attack has been conducted on our server.

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20389	192.168.75.137	23	
2	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20389	
3	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20389	192.168.75.137	23	
4	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20390	192.168.75.137	23	
5	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20391	192.168.75.137	23	
6	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20390	
7	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20390	192.168.75.137	23	
8	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20391	
9	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20391	192.168.75.137	23	
10	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20392	192.168.75.137	23	
11	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20392	
12	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20392	192.168.75.137	23	
13	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20393	192.168.75.137	23	
14	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20393	
15	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20393	192.168.75.137	23	
16	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20394	192.168.75.137	23	
17	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20394	
18	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20394	192.168.75.137	23	
19	TCP	S----	04/01/2010 10:33:09	192.168.75.1	20395	192.168.75.137	23	
20	TCP	SA---	04/01/2010 10:33:09	192.168.75.137	23	192.168.75.1	20395	
21	TCP	-A---	04/01/2010 10:33:09	192.168.75.1	20395	192.168.75.137	23	

Figure 1.9: Hydra\_telnet dump

Determine the following:

**Sending src TCP port range:**

**Receiver src TCP port:**

**Sending src IP address:**

**Receiver src IP address:**

**What are the logins used:**

**What are the passwords used:**

**What is the successful login/password:**

1.10 Open **hping\_udp\_scan** dump (see Figure 1.10).

No.	Type	Flags	Time	Source IP	Source Port	Dest IP	Dest Port	Content
1	UDP		04/01/2010 10:40:05	192.168.75.138	2228	192.168.75.1	0	eth0
2	UDP		04/01/2010 10:40:06	192.168.75.138	2229	192.168.75.1	0	eth0
3	UDP		04/01/2010 10:40:07	192.168.75.138	2230	192.168.75.1	0	eth0
4	UDP		04/01/2010 10:40:08	192.168.75.138	2231	192.168.75.1	0	eth0
5	UDP		04/01/2010 10:40:09	192.168.75.138	2232	192.168.75.1	0	eth0
6	ARP	ARP ...	04/01/2010 10:40:10	MAC:00:0c:29:6b:0e:96		MAC:00:00:00:00:00:00		
7	ARP	ARP ...	04/01/2010 10:40:10	MAC:00:50:56:c0:00:08		MAC:00:0c:29:6b:0e:96		
8	UDP		04/01/2010 10:40:10	192.168.75.138	2233	192.168.75.1	0	eth0
9	UDP		04/01/2010 10:40:11	192.168.75.138	5353	224.0.0.251	5353	~~~~~...
10	UDP		04/01/2010 10:40:11	192.168.75.138	2234	192.168.75.1	0	eth0
11	UDP		04/01/2010 10:40:12	192.168.75.138	2235	192.168.75.1	0	eth0
12	UDP		04/01/2010 10:40:13	192.168.75.138	2236	192.168.75.1	0	eth0
13	UDP		04/01/2010 10:40:14	192.168.75.138	2237	192.168.75.1	0	eth0
14	UDP		04/01/2010 10:40:15	192.168.75.138	2238	192.168.75.1	0	eth0
15	UDP		04/01/2010 10:40:16	192.168.75.138	2239	192.168.75.1	0	eth0
16	UDP		04/01/2010 10:40:17	192.168.75.138	2240	192.168.75.1	0	eth0
17	UDP		04/01/2010 10:40:18	192.168.75.138	2241	192.168.75.1	0	eth0
18	UDP		04/01/2010 10:40:19	192.168.75.138	2242	192.168.75.1	0	eth0
19	UDP		04/01/2010 10:40:20	192.168.75.138	2243	192.168.75.1	0	eth0
20	UDP		04/01/2010 10:40:21	192.168.75.138	2244	192.168.75.1	0	eth0
21	UDP		04/01/2010 10:40:22	192.168.75.138	2245	192.168.75.1	0	eth0

Figure 1.10: Hping\_UDP\_scan

Determine the following:

**Sending src UDP port range:**

**Receiver src UDP port:**

**Sending src IP address:**

**Receiver src IP address:**