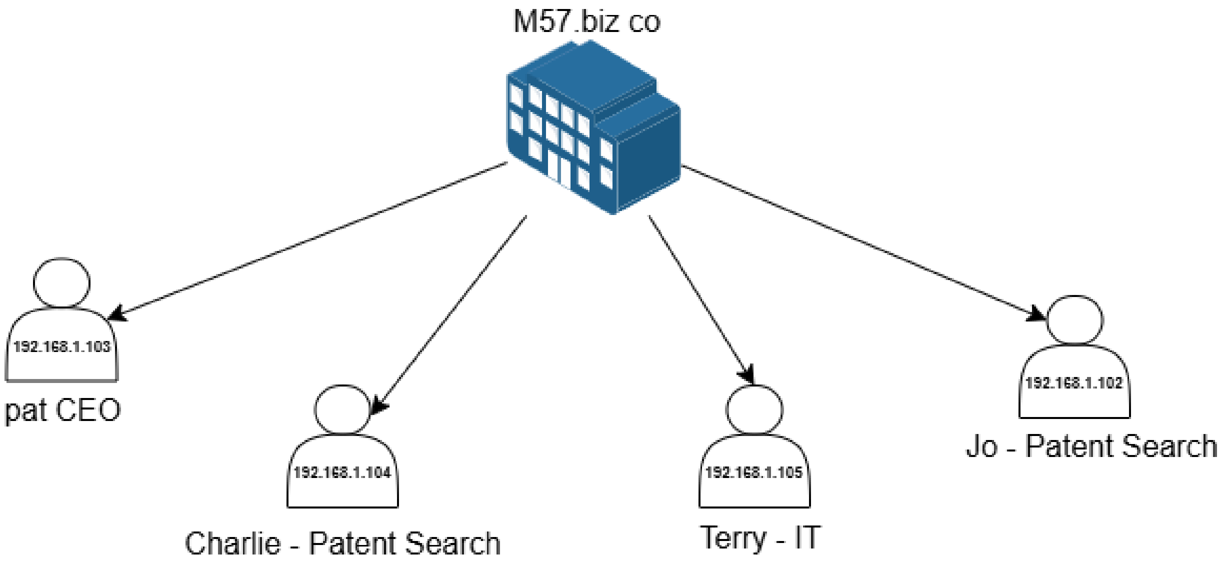
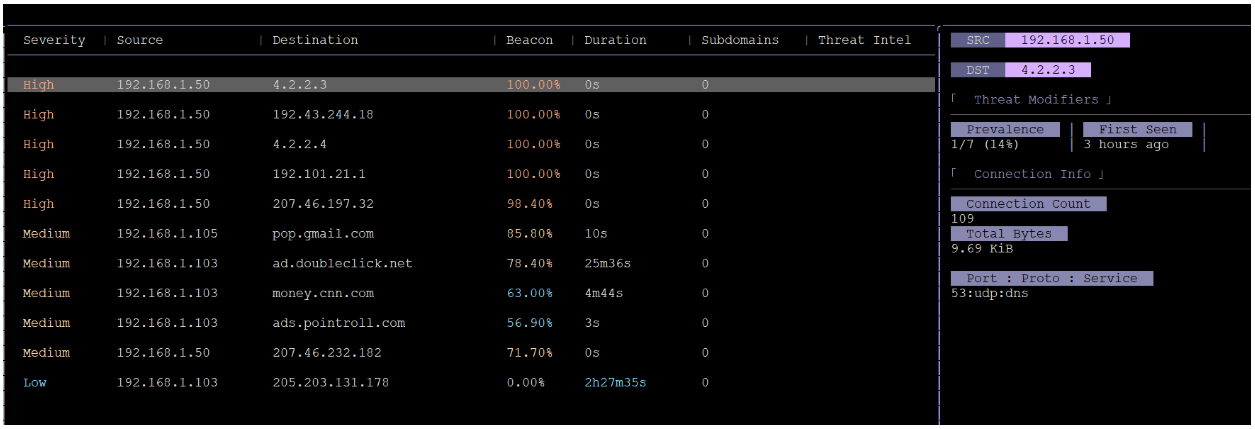
Results of the Investigation into the M57 Patents Breach Between November 13, 2009, and December 12, 2009, **M57 Patents**, a fast-growing startup specializing in outsourced patent research, experienced rapid expansion. However, within less than a month of operations, the company faced internal threats, suspicious network activities, and potential data exfiltration attempts, ultimately leading to its downfall.

During my investigation of **Week 1 only (Nov 16–20, 2009)**, I uncovered substantial evidence indicating **unauthorized access**, **data exfiltration**, **malicious insider activity**



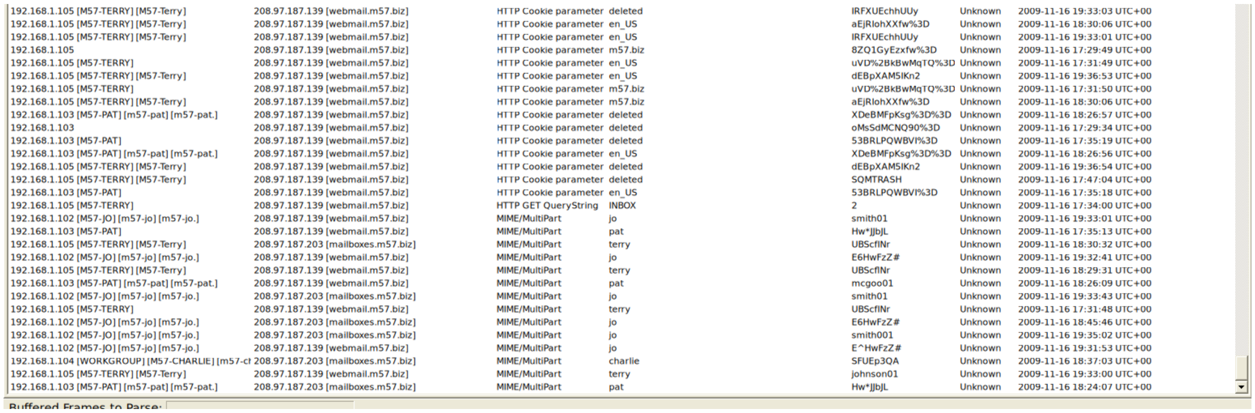
net-2009-11-16-09-24.pcap



```
 Severity | Source        | Destination        | Beacon  | Duration  | Subdomains | Threat Intel     SRC  192.168.1.50

                                                                                                      DST  4.2.2.3
 High       192.168.1.50    4.2.2.3              100.00%   0s          0
                                                                                                      ⌜ Threat Modifiers ⌟
 High       192.168.1.50    192.43.244.18        100.00%   0s          0
                                                                                                      Prevalence  | First Seen  |
 High       192.168.1.50    4.2.2.4              100.00%   0s          0                              1/7 (14%)   | 3 hours ago |

 High       192.168.1.50    192.101.21.1         100.00%   0s          0                              ⌜ Connection Info ⌟

 High       192.168.1.50    207.46.197.32        98.40%    0s          0                              Connection Count
                                                                                                      109
 Medium     192.168.1.105   pop.gmail.com        85.80%    10s         0                              Total Bytes
                                                                                                      9.69 KiB
 Medium     192.168.1.103   ad.doubleclick.net   78.40%    25m36s      0
                                                                                                      Port : Proto : Service
 Medium     192.168.1.103   money.cnn.com        63.00%    4m44s       0                              53:udp:dns

 Medium     192.168.1.103   ads.pointroll.com    56.90%    3s          0

 Medium     192.168.1.50    207.46.232.182       71.70%    0s          0

 Low        192.168.1.103   205.203.131.178      0.00%     2h27m35s    0
```

High-risk connections were identified between the internal device **192.168.1.50** and several suspicious servers, including **4.2.2.3** and **207.46.197.32**, via the **DNS protocol**.

These connections represent unauthorized data transfer, which may be linked to **data exfiltration** or an attempt to **infiltrate the network**.

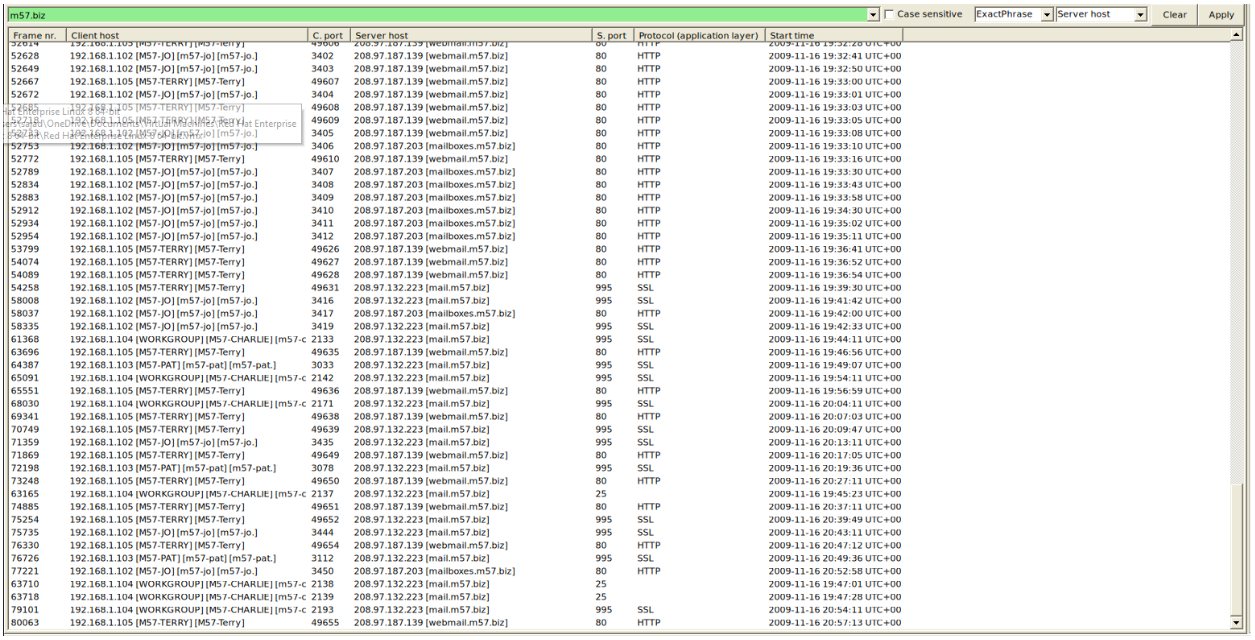


```
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   IRFXUEchhUUy        Unknown  2009-11-16 19:33:03 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     aEjRlohXXfw%3D      Unknown  2009-11-16 18:30:06 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     IRFXUEchhUUy        Unknown  2009-11-16 19:33:01 UTC+00
192.168.1.105                                   208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  m57.biz   8ZQ1GyEzxfw%3D      Unknown  2009-11-16 17:29:49 UTC+00
192.168.1.105 [M57-TERRY]                       208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     uVD%2BkBwMqTQ%3D    Unknown  2009-11-16 17:31:49 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     dEBpXAM5IKn2        Unknown  2009-11-16 19:36:53 UTC+00
192.168.1.105 [M57-TERRY]                       208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  m57.biz   uVD%2BkBwMqTQ%3D    Unknown  2009-11-16 17:31:50 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  m57.biz   aEjRlohXXfw%3D      Unknown  2009-11-16 18:30:06 UTC+00
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]    208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   XDeBMFpKsg%3D%3D    Unknown  2009-11-16 18:26:57 UTC+00
192.168.1.103                                   208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   oMsSdMCNQ90%3D      Unknown  2009-11-16 17:29:34 UTC+00
192.168.1.103 [M57-PAT]                         208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   53BRLPQWBVI%3D      Unknown  2009-11-16 17:35:19 UTC+00
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]    208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     XDeBMFpKsg%3D%3D    Unknown  2009-11-16 18:26:56 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   dEBpXAM5IKn2        Unknown  2009-11-16 19:36:54 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  deleted   SQMTRASH            Unknown  2009-11-16 17:47:04 UTC+00
192.168.1.103 [M57-PAT]                         208.97.187.139 [webmail.m57.biz]    HTTP Cookie parameter  en_US     53BRLPQWBVI%3D      Unknown  2009-11-16 17:35:18 UTC+00
192.168.1.105 [M57-TERRY]                       208.97.187.139 [webmail.m57.biz]    HTTP GET QueryString   INBOX     2                   Unknown  2009-11-16 17:34:00 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         jo        smith01             Unknown  2009-11-16 19:33:01 UTC+00
192.168.1.103 [M57-PAT]                         208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         pat       Hw*JJbJL            Unknown  2009-11-16 17:35:13 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         terry     UBScflNr            Unknown  2009-11-16 18:30:32 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         jo        E6HwFzZ#            Unknown  2009-11-16 19:32:41 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         terry     UBScflNr            Unknown  2009-11-16 18:29:31 UTC+00
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]    208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         pat       mcgoo01             Unknown  2009-11-16 18:26:09 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         jo        smith01             Unknown  2009-11-16 19:33:43 UTC+00
192.168.1.105 [M57-TERRY]                       208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         terry     UBScflNr            Unknown  2009-11-16 17:31:48 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         jo        E6HwFzZ#            Unknown  2009-11-16 18:45:46 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         jo        smith001            Unknown  2009-11-16 19:35:02 UTC+00
192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]       208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         jo        E^HwFzZ#            Unknown  2009-11-16 19:31:53 UTC+00
192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-ch 208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         charlie   SFUEp3QA            Unknown  2009-11-16 18:37:03 UTC+00
192.168.1.105 [M57-TERRY] [M57-Terry]           208.97.187.139 [webmail.m57.biz]    MIME/MultiPart         terry     johnson01           Unknown  2009-11-16 19:33:00 UTC+00
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]    208.97.187.203 [mailboxes.m57.biz]  MIME/MultiPart         pat       Hw*JJbJL            Unknown  2009-11-16 18:24:07 UTC+00
Buffered Frames to Parse:
```

Exposed passwords for several employees, such as **terry**, **jo**, and **pat**, were discovered.

This data was leaked through **HTTP** and **MIME/Multipart** traffic, indicating a potential **internal breach** or an **attack on employee accounts**.

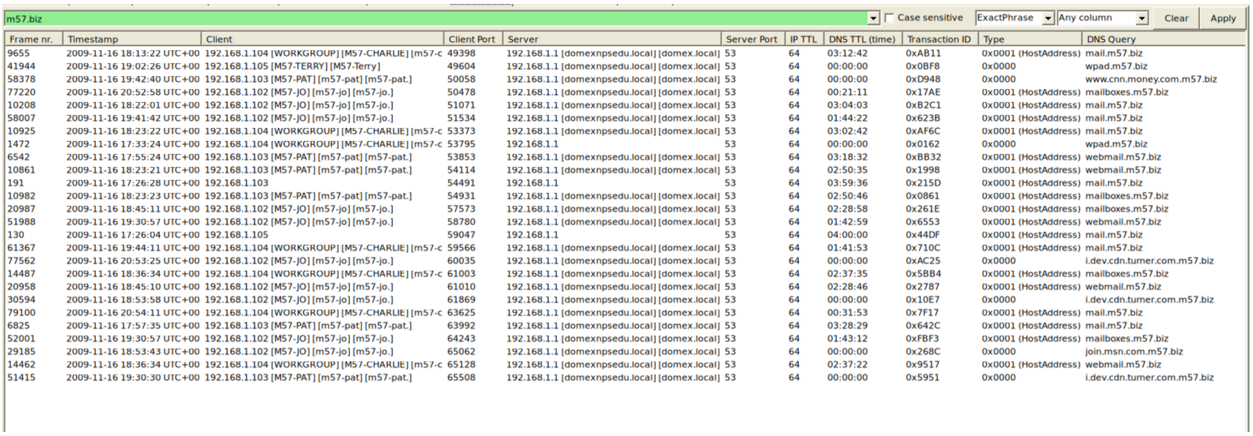
By sajad hasan ali


m57.biz
☐ Case sensitive
ExactPhrase
Server host
Clear
Apply
at Enterprise Linux 8 64-bit
ers\sajad\OneDrive\Documents\Virtual Machines\Red Hat Enterprise
8 64-bit\Red Hat Enterprise Linux 8 64-bit.vmx

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
52614	192.168.1.105 [M57-TERRY] [M57-Terry]	49606	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:32:28 UTC+00
52628	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3402	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:32:41 UTC+00
52649	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3403	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:32:50 UTC+00
52667	192.168.1.105 [M57-TERRY] [M57-Terry]	49607	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:00 UTC+00
52672	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3404	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:01 UTC+00
52685	192.168.1.105 [M57-TERRY] [M57-Terry]	49608	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:03 UTC+00
52718	192.168.1.105 [M57-TERRY] [M57-Terry]	49609	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:05 UTC+00
52733	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3405	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:08 UTC+00
52753	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3406	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:33:10 UTC+00
52772	192.168.1.105 [M57-TERRY] [M57-Terry]	49610	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:33:16 UTC+00
52789	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3407	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:33:30 UTC+00
52834	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3408	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:33:43 UTC+00
52883	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3409	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:33:58 UTC+00
52912	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3410	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:34:30 UTC+00
52934	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3411	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:35:02 UTC+00
52954	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3412	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:35:11 UTC+00
53799	192.168.1.105 [M57-TERRY] [M57-Terry]	49626	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:36:41 UTC+00
54074	192.168.1.105 [M57-TERRY] [M57-Terry]	49627	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:36:52 UTC+00
54089	192.168.1.105 [M57-TERRY] [M57-Terry]	49628	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:36:54 UTC+00
54258	192.168.1.105 [M57-TERRY] [M57-Terry]	49631	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:39:30 UTC+00
58008	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3416	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:41:42 UTC+00
58037	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3417	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 19:42:00 UTC+00
58335	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3419	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:42:33 UTC+00
61368	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2133	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:44:11 UTC+00
63696	192.168.1.105 [M57-TERRY] [M57-Terry]	49635	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:46:56 UTC+00
64387	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	3033	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:49:07 UTC+00
65091	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2142	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 19:54:11 UTC+00
65551	192.168.1.105 [M57-TERRY] [M57-Terry]	49636	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 19:56:59 UTC+00
68030	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2171	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:04:11 UTC+00
69341	192.168.1.105 [M57-TERRY] [M57-Terry]	49638	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:07:03 UTC+00
70749	192.168.1.105 [M57-TERRY] [M57-Terry]	49639	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:09:47 UTC+00
71359	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3435	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:13:11 UTC+00
71869	192.168.1.105 [M57-TERRY] [M57-Terry]	49649	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:17:05 UTC+00
72198	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	3078	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:19:36 UTC+00
73248	192.168.1.105 [M57-TERRY] [M57-Terry]	49650	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:27:11 UTC+00
63165	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2137	208.97.132.223 [mail.m57.biz]	25		2009-11-16 19:45:23 UTC+00
74885	192.168.1.105 [M57-TERRY] [M57-Terry]	49651	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:37:11 UTC+00
75254	192.168.1.105 [M57-TERRY] [M57-Terry]	49652	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:39:49 UTC+00
75735	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3444	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:43:11 UTC+00
76330	192.168.1.105 [M57-TERRY] [M57-Terry]	49654	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:47:12 UTC+00
76726	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	3112	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:49:36 UTC+00
77221	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	3450	208.97.187.203 [mailboxes.m57.biz]	80	HTTP	2009-11-16 20:52:58 UTC+00
63710	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2138	208.97.132.223 [mail.m57.biz]	25		2009-11-16 19:47:01 UTC+00
63718	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2139	208.97.132.223 [mail.m57.biz]	25		2009-11-16 19:47:28 UTC+00
79101	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	2193	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-16 20:54:11 UTC+00
80063	192.168.1.105 [M57-TERRY] [M57-Terry]	49655	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-16 20:57:13 UTC+00

Multiple sessions were recorded between internal devices, such as **192.168.1.103**, **192.168.1.102**, **192.168.1.104**, and **192.168.1.105**, and external servers like **webmail.m57.biz** and **mailboxes.m57.biz**.

The repeated connection to these servers suggests suspicious activity, potentially related to **data exfiltration attempts** or **persistent infiltration attempts** across the network.

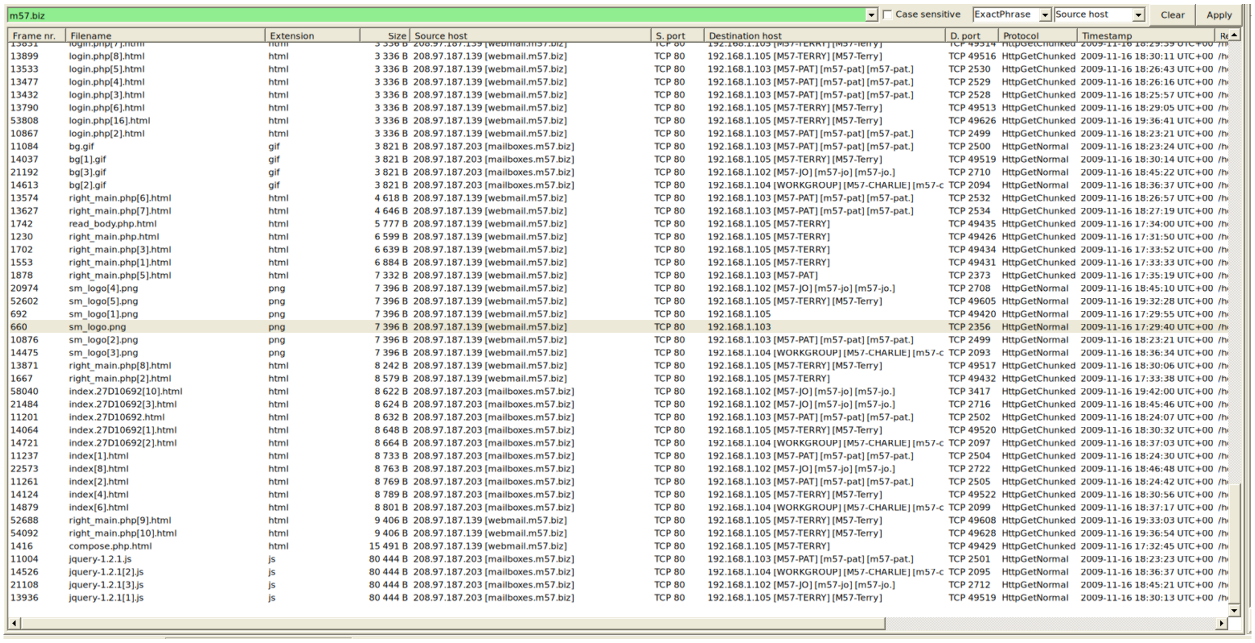


Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query
9655	2009-11-16 18:13:22 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	49398	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:12:42	0xAB11	0x0001 (HostAddress)	mail.m57.biz
41944	2009-11-16 19:02:26 UTC+00	192.168.1.105 [M57-TERRY] [M57-Terry]	49604	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x0BF8	0x0000	wpad.m57.biz
58378	2009-11-16 19:42:40 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	50058	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xD948	0x0000	www.cnn.money.com.m57.biz
77220	2009-11-16 20:52:58 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	50478	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:21:11	0x17AE	0x0001 (HostAddress)	mailboxes.m57.biz
10208	2009-11-16 18:22:01 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	51071	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:04:03	0xB2C1	0x0001 (HostAddress)	mail.m57.biz
58007	2009-11-16 19:41:42 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	51534	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:44:22	0x623B	0x0001 (HostAddress)	mail.m57.biz
10925	2009-11-16 18:23:22 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	53373	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:02:42	0xAF6C	0x0001 (HostAddress)	mail.m57.biz
1472	2009-11-16 17:33:24 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	53795	192.168.1.1	53	64	00:00:00	0x0162	0x0000	wpad.m57.biz
6542	2009-11-16 17:55:24 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	53853	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:18:32	0xBB32	0x0001 (HostAddress)	webmail.m57.biz
10861	2009-11-16 18:23:21 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	54114	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:50:35	0x1998	0x0001 (HostAddress)	webmail.m57.biz
191	2009-11-16 17:26:28 UTC+00	192.168.1.103	54491	192.168.1.1	53	64	03:59:36	0x215D	0x0001 (HostAddress)	mail.m57.biz
10982	2009-11-16 18:23:23 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	54931	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:50:46	0x0861	0x0001 (HostAddress)	mailboxes.m57.biz
20987	2009-11-16 18:45:11 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	57573	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:28:58	0x261E	0x0001 (HostAddress)	mailboxes.m57.biz
51988	2009-11-16 19:30:57 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	58780	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:42:59	0x6553	0x0001 (HostAddress)	webmail.m57.biz
130	2009-11-16 17:26:04 UTC+00	192.168.1.105	59047	192.168.1.1	53	64	04:00:00	0x44DF	0x0001 (HostAddress)	mail.m57.biz
61367	2009-11-16 19:44:11 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	59566	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:41:53	0x710C	0x0001 (HostAddress)	mail.m57.biz
77562	2009-11-16 20:53:25 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	60035	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xAC25	0x0000	i.dev.cdn.turner.com.m57.biz
14487	2009-11-16 18:36:34 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	61003	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:37:35	0x5BB4	0x0001 (HostAddress)	mailboxes.m57.biz
20958	2009-11-16 18:45:10 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	61010	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:28:46	0x2787	0x0001 (HostAddress)	webmail.m57.biz
30594	2009-11-16 18:53:58 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	61869	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x10E7	0x0000	i.dev.cdn.turner.com.m57.biz
79100	2009-11-16 20:54:11 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	63625	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:31:53	0x7F17	0x0001 (HostAddress)	mail.m57.biz
6825	2009-11-16 17:57:35 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	63992	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:28:29	0x642C	0x0001 (HostAddress)	mail.m57.biz
52001	2009-11-16 19:30:57 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	64243	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:43:12	0xFBF3	0x0001 (HostAddress)	mailboxes.m57.biz
29185	2009-11-16 18:53:43 UTC+00	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	65062	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x268C	0x0000	join.msn.com.m57.biz
14462	2009-11-16 18:36:34 UTC+00	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	65128	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:37:22	0x9517	0x0001 (HostAddress)	webmail.m57.biz
51415	2009-11-16 19:30:30 UTC+00	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	65508	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x5951	0x0000	i.dev.cdn.turner.com.m57.biz

Suspicious **DNS queries** were detected from internal devices to untrusted external servers, such as **webmail.m57.biz** and **mailboxes.m57.biz**.

The repetition of these queries over the **DNS protocol** (port 53) suggests a potential **data leakage** or an **unauthorized attempt to connect** to external monitoring servers.

By sajad hasan ali

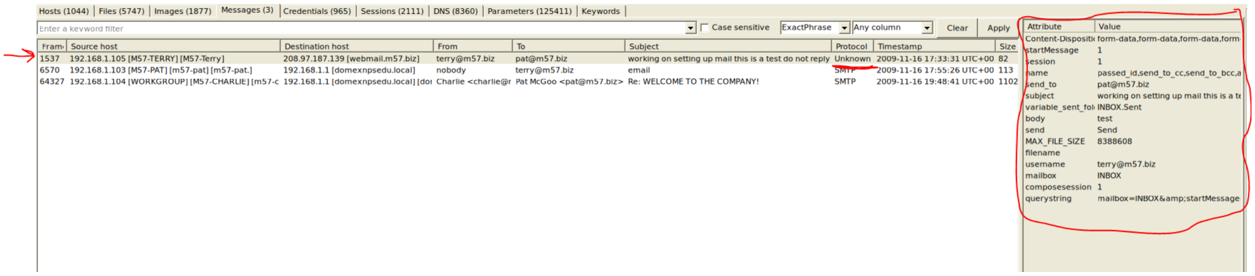


m57.biz ☐ Case sensitive ExactPhrase Source host

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Re
13831	login.php[7].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49514	HttpGetChunked	2009-11-16 18:29:39 UTC+00	/h
13899	login.php[8].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49516	HttpGetChunked	2009-11-16 18:30:11 UTC+00	/h
13533	login.php[5].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2530	HttpGetChunked	2009-11-16 18:26:43 UTC+00	/h
13477	login.php[4].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2529	HttpGetChunked	2009-11-16 18:26:16 UTC+00	/h
13432	login.php[3].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2528	HttpGetChunked	2009-11-16 18:25:57 UTC+00	/h
13790	login.php[6].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49513	HttpGetChunked	2009-11-16 18:29:05 UTC+00	/h
53808	login.php[16].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49626	HttpGetChunked	2009-11-16 19:36:41 UTC+00	/h
10867	login.php[2].html	html	3 336 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2499	HttpGetChunked	2009-11-16 18:23:21 UTC+00	/h
11084	bg.gif	gif	3 821 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2500	HttpGetNormal	2009-11-16 18:23:24 UTC+00	/h
14037	bg[1].gif	gif	3 821 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49519	HttpGetNormal	2009-11-16 18:30:14 UTC+00	/h
21192	bg[3].gif	gif	3 821 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 2710	HttpGetNormal	2009-11-16 18:45:22 UTC+00	/h
14613	bg[2].gif	gif	3 821 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	TCP 2094	HttpGetNormal	2009-11-16 18:36:37 UTC+00	/h
13574	right_main.php[6].html	html	4 618 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2532	HttpGetChunked	2009-11-16 18:26:57 UTC+00	/h
13627	right_main.php[7].html	html	4 646 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2534	HttpGetChunked	2009-11-16 18:27:19 UTC+00	/h
1742	read_body.php.html	html	5 777 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49435	HttpGetChunked	2009-11-16 17:34:00 UTC+00	/h
1230	right_main.php.html	html	6 599 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49426	HttpGetChunked	2009-11-16 17:31:50 UTC+00	/h
1702	right_main.php[3].html	html	6 639 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49434	HttpGetChunked	2009-11-16 17:33:52 UTC+00	/h
1553	right_main.php[1].html	html	6 884 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49431	HttpGetChunked	2009-11-16 17:33:33 UTC+00	/h
1878	right_main.php[5].html	html	7 332 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT]	TCP 2373	HttpGetChunked	2009-11-16 17:35:19 UTC+00	/h
20974	sm_logo[4].png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 2708	HttpGetNormal	2009-11-16 18:45:10 UTC+00	/h
52602	sm_logo[5].png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49605	HttpGetNormal	2009-11-16 19:32:28 UTC+00	/h
692	sm_logo[1].png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105	TCP 49420	HttpGetNormal	2009-11-16 17:29:55 UTC+00	/h
660	sm_logo.png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103	TCP 2356	HttpGetNormal	2009-11-16 17:29:40 UTC+00	/h
10876	sm_logo[2].png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2499	HttpGetNormal	2009-11-16 18:23:21 UTC+00	/h
14475	sm_logo[3].png	png	7 396 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	TCP 2093	HttpGetNormal	2009-11-16 18:36:34 UTC+00	/h
13871	right_main.php[8].html	html	8 242 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49517	HttpGetChunked	2009-11-16 18:30:06 UTC+00	/h
1667	right_main.php[2].html	html	8 579 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49432	HttpGetChunked	2009-11-16 17:33:38 UTC+00	/h
58040	index.27D10692[10].html	html	8 622 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 3417	HttpGetChunked	2009-11-16 19:42:00 UTC+00	/h
21484	index.27D10692[3].html	html	8 624 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 2716	HttpGetChunked	2009-11-16 18:45:46 UTC+00	/h
11201	index.27D10692.html	html	8 632 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2502	HttpGetChunked	2009-11-16 18:24:07 UTC+00	/h
14064	index.27D10692[1].html	html	8 648 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49520	HttpGetChunked	2009-11-16 18:30:32 UTC+00	/h
14721	index.27D10692[2].html	html	8 664 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	TCP 2097	HttpGetChunked	2009-11-16 18:37:03 UTC+00	/h
11237	index[1].html	html	8 733 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2504	HttpGetChunked	2009-11-16 18:24:30 UTC+00	/h
22573	index[8].html	html	8 763 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 2722	HttpGetChunked	2009-11-16 18:46:48 UTC+00	/h
11261	index[2].html	html	8 769 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2505	HttpGetChunked	2009-11-16 18:24:42 UTC+00	/h
14124	index[4].html	html	8 789 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49522	HttpGetChunked	2009-11-16 18:30:56 UTC+00	/h
14879	index[6].html	html	8 801 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	TCP 2099	HttpGetChunked	2009-11-16 18:37:17 UTC+00	/h
52688	right_main.php[9].html	html	9 406 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49608	HttpGetChunked	2009-11-16 19:33:03 UTC+00	/h
54092	right_main.php[10].html	html	9 406 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49628	HttpGetChunked	2009-11-16 19:36:54 UTC+00	/h
1416	compose.php.html	html	15 491 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49429	HttpGetChunked	2009-11-16 17:32:45 UTC+00	/h
11004	jquery-1.2.1.js	js	80 444 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	TCP 2501	HttpGetNormal	2009-11-16 18:23:23 UTC+00	/h
14526	jquery-1.2.1[2].js	js	80 444 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	TCP 2095	HttpGetNormal	2009-11-16 18:36:37 UTC+00	/h
21108	jquery-1.2.1[3].js	js	80 444 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	TCP 2712	HttpGetNormal	2009-11-16 18:45:21 UTC+00	/h
13936	jquery-1.2.1[1].js	js	80 444 B	208.97.187.203 [mailboxes.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry]	TCP 49519	HttpGetNormal	2009-11-16 18:30:13 UTC+00	/h

Suspicious files were downloaded via **HTTP protocols** from **webmail.m57.biz** and **mailboxes.m57.biz**.

These files included **HTML**, **PNG**, and **JS** formats, indicating attempts to implant **malicious code** or exfiltrate **sensitive data** through email attachments.



☐ Case sensitive ExactPhrase Any column

Fram	Source host	Destination host	From	To	Subject	Protocol	Timestamp	Size
1537	192.168.1.105 [M57-TERRY] [M57-Terry]	208.97.187.139 [webmail.m57.biz]	terry@m57.biz	pat@m57.biz	working on setting up mail this is a test do not reply	Unknown	2009-11-16 17:33:31 UTC+00	82
6570	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	192.168.1.1 [domexnpsedu.local]	nobody	terry@m57.biz	email	SMTP	2009-11-16 17:55:26 UTC+00	113
64327	192.168.1.104 [WORKGROUP] [M57-CHARLIE] [m57-c	192.168.1.1 [domexnpsedu.local] [do	Charlie <charlie@r	Pat McGoo <pat@m57.biz>	Re: WELCOME TO THE COMPANY!	SMTP	2009-11-16 19:48:41 UTC+00	1102

Attribute	Value
Content-Dispositi	form-data,form-data,form-data,form-
startMessage	1
session	1
name	passed_id,send_to_cc,send_to_bcc,a
send_to	pat@m57.biz
subject	working on setting up mail this is a te
variable_sent_fol	INBOX.Sent
body	test
send	Send
MAX_FILE_SIZE	8388608
filename	
username	terry@m57.biz
mailbox	INBOX
composesession	1
querystring	mailbox=INBOX&amp;startMessage

A suspicious message was detected, sent from **terry@m57.biz** to **pat@m57.biz** with the subject "working on setting up mail this is a test do not reply."

This message may contain **malicious files** or **stolen data**, sent in an attempt to **conceal harmful activities**. It was transmitted via an **unknown protocol**.

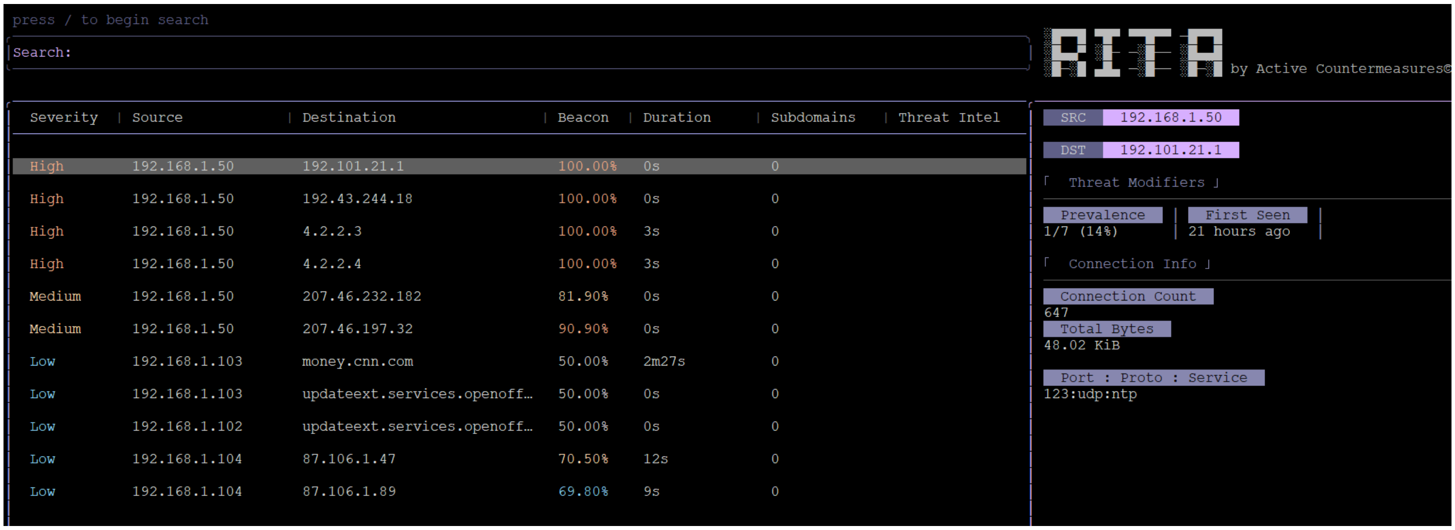
By sajad hasan ali

Recommended Actions:

1. Review and analyze the attachments in suspicious messages (such as those delivered via HTTP and MIME/Multipart).
2. Immediately change passwords for all affected employees, especially those whose passwords have been exposed.
3. Isolate affected devices, such as **192.168.1.50**, from the network to investigate suspicious activities.
4. Block all **DNS queries** to **webmail.m57.biz** and **mailboxes.m57.biz**, along with other connections to suspicious servers.
5. Conduct a security review across internal systems to implement stricter security filters and regularly check logs.
6. Monitor accounts at risk of compromise, such as **terry**, **jo**, and **pat**.

By sajad hasan ali

net-2009-11-16-13-08.pcap

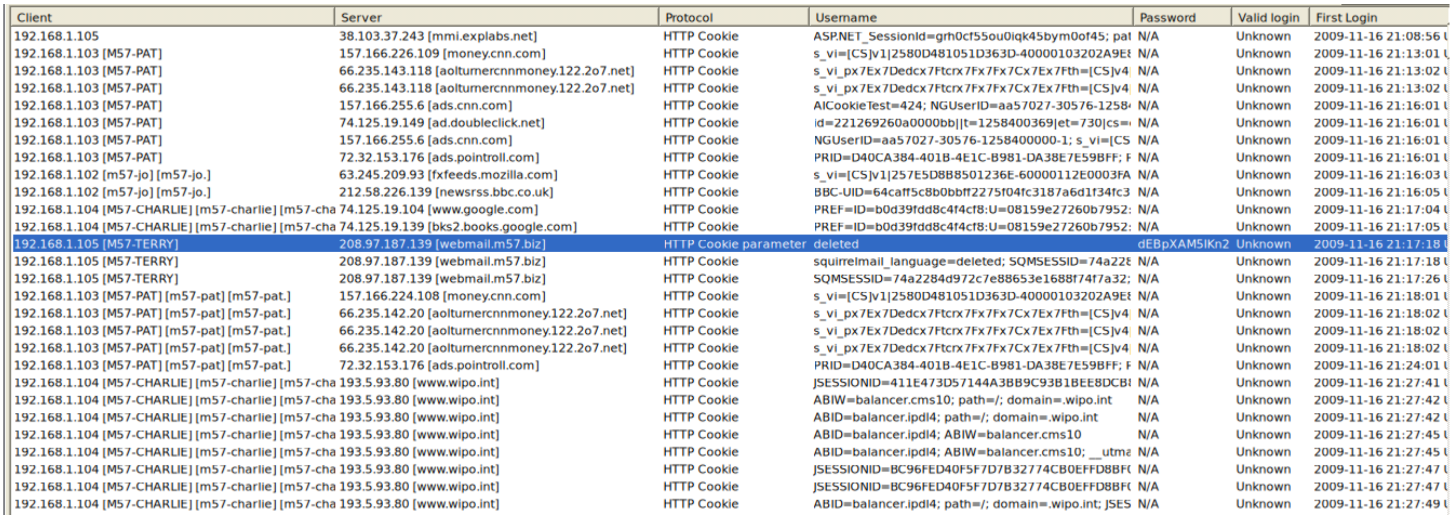


```
press / to begin search
Search:
                                                                                  RITA by Active Countermeasures©
 Severity | Source          | Destination                  | Beacon  | Duration | Subdomains | Threat Intel    SRC  192.168.1.50
                                                                                                              DST  192.101.21.1
 High       192.168.1.50      192.101.21.1                   100.00%   0s         0                           ┌ Threat Modifiers ┘
 High       192.168.1.50      192.43.244.18                  100.00%   0s         0                           Prevalence    | First Seen
 High       192.168.1.50      4.2.2.3                        100.00%   3s         0                           1/7 (14%)     | 21 hours ago
 High       192.168.1.50      4.2.2.4                        100.00%   3s         0                           ┌ Connection Info ┘
 Medium     192.168.1.50      207.46.232.182                 81.90%    0s         0                           Connection Count
 Medium     192.168.1.50      207.46.197.32                  90.90%    0s         0                           647
 Low        192.168.1.103     money.cnn.com                  50.00%    2m27s      0                           Total Bytes
 Low        192.168.1.103     updateext.services.openoff…    50.00%    0s         0                           48.02 KiB
 Low        192.168.1.102     updateext.services.openoff…    50.00%    0s         0                           Port : Proto : Service
 Low        192.168.1.104     87.106.1.47                    70.50%    12s        0                           123:udp:ntp
 Low        192.168.1.104     87.106.1.89                    69.80%    9s         0
```

Zeek and RITA Analysis:

- **High-Risk Connections:** Suspicious high-risk communications were detected between the internal device (**192.168.1.50**) and several **external IP addresses**. These connections suggest abnormal interaction with external servers, which may indicate a potential **data exfiltration attempt** or an **external cyberattack**.

- **Isolation Action:** The device **192.168.1.50** was isolated due to transmitting **a large volume of data** to external servers, raising serious concerns about a potential data breach.



Client	Server	Protocol	Username	Password	Valid login	First Login
192.168.1.105	38.103.37.243 [mmi.explabs.net]	HTTP Cookie	ASP.NET_SessionId=grh0cf55ou0iqk45bym0of45; pat	N/A	Unknown	2009-11-16 21:08:56
192.168.1.103 [M57-PAT]	157.166.226.109 [money.cnn.com]	HTTP Cookie	s_vi=[CS]v1|2580D481051D363D-40000103202A9E	N/A	Unknown	2009-11-16 21:13:01
192.168.1.103 [M57-PAT]	66.235.143.118 [aolturnercnnmoney.122.2o7.net]	HTTP Cookie	s_vi_px7Ex7Dedcx7Ftcrx7Fx7Fx7Cx7Ex7Fth=[CS]v4	N/A	Unknown	2009-11-16 21:13:02
192.168.1.103 [M57-PAT]	66.235.143.118 [aolturnercnnmoney.122.2o7.net]	HTTP Cookie	s_vi_px7Ex7Dedcx7Ftcrx7Fx7Fx7Cx7Ex7Fth=[CS]v4	N/A	Unknown	2009-11-16 21:13:02
192.168.1.103 [M57-PAT]	157.166.255.6 [ads.cnn.com]	HTTP Cookie	AICookieTest=424; NGUserID=aa57027-30576-1258	N/A	Unknown	2009-11-16 21:16:01
192.168.1.103 [M57-PAT]	74.125.19.149 [ad.doubleclick.net]	HTTP Cookie	id=221269260a0000bb||t=1258400369|et=730|cs=	N/A	Unknown	2009-11-16 21:16:01
192.168.1.103 [M57-PAT]	157.166.255.6 [ads.cnn.com]	HTTP Cookie	NGUserID=aa57027-30576-1258400000-1; s_vi=[CS	N/A	Unknown	2009-11-16 21:16:01
192.168.1.103 [M57-PAT]	72.32.153.176 [ads.pointroll.com]	HTTP Cookie	PRID=D40CA384-401B-4E1C-B981-DA38E7E59BFF; F	N/A	Unknown	2009-11-16 21:16:01
192.168.1.102 [m57-jo] [m57-jo.]	63.245.209.93 [fxfeeds.mozilla.com]	HTTP Cookie	s_vi=[CS]v1|257E5D8B8501236E-60000112E0003FA	N/A	Unknown	2009-11-16 21:16:03
192.168.1.102 [m57-jo] [m57-jo.]	212.58.226.139 [newsrss.bbc.co.uk]	HTTP Cookie	BBC-UID=64caff5c8b0bbff2275f04fc3187a6d1f34fc3	N/A	Unknown	2009-11-16 21:16:05
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.19.104 [www.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11-16 21:17:04
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.19.139 [bks2.books.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11-16 21:17:05
192.168.1.105 [M57-TERRY]	208.97.187.139 [webmail.m57.biz]	HTTP Cookie parameter	deleted	dEBpXAM5IKn2	Unknown	2009-11-16 21:17:18
192.168.1.105 [M57-TERRY]	208.97.187.139 [webmail.m57.biz]	HTTP Cookie	squirrelmail_language=deleted; SQMSESSID=74a22	N/A	Unknown	2009-11-16 21:17:18
192.168.1.105 [M57-TERRY]	208.97.187.139 [webmail.m57.biz]	HTTP Cookie	SQMSESSID=74a2284d972c7e88653e1688f74f7a32;	N/A	Unknown	2009-11-16 21:17:26
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	157.166.224.108 [money.cnn.com]	HTTP Cookie	s_vi=[CS]v1|2580D481051D363D-40000103202A9E	N/A	Unknown	2009-11-16 21:18:01
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	66.235.142.20 [aolturnercnnmoney.122.2o7.net]	HTTP Cookie	s_vi_px7Ex7Dedcx7Ftcrx7Fx7Fx7Cx7Ex7Fth=[CS]v4	N/A	Unknown	2009-11-16 21:18:02
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	66.235.142.20 [aolturnercnnmoney.122.2o7.net]	HTTP Cookie	s_vi_px7Ex7Dedcx7Ftcrx7Fx7Fx7Cx7Ex7Fth=[CS]v4	N/A	Unknown	2009-11-16 21:18:02
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	66.235.142.20 [aolturnercnnmoney.122.2o7.net]	HTTP Cookie	s_vi_px7Ex7Dedcx7Ftcrx7Fx7Fx7Cx7Ex7Fth=[CS]v4	N/A	Unknown	2009-11-16 21:18:02
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	72.32.153.176 [ads.pointroll.com]	HTTP Cookie	PRID=D40CA384-401B-4E1C-B981-DA38E7E59BFF; F	N/A	Unknown	2009-11-16 21:24:01
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	JSESSIONID=411E473D57144A3BB9C93B1BEE8DCB	N/A	Unknown	2009-11-16 21:27:41
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	ABIW=balancer.cms10; path=/; domain=.wipo.int	N/A	Unknown	2009-11-16 21:27:42
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	ABID=balancer.ipdl4; path=/; domain=.wipo.int	N/A	Unknown	2009-11-16 21:27:42
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	ABID=balancer.ipdl4; ABIW=balancer.cms10	N/A	Unknown	2009-11-16 21:27:45
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	ABID=balancer.ipdl4; ABIW=balancer.cms10; __utma	N/A	Unknown	2009-11-16 21:27:45
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	JSESSIONID=BC96FED40F5F7D7B32774CB0EFFD8BF	N/A	Unknown	2009-11-16 21:27:47
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	JSESSIONID=BC96FED40F5F7D7B32774CB0EFFD8BF	N/A	Unknown	2009-11-16 21:27:47
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	193.5.93.80 [www.wipo.int]	HTTP Cookie	ABID=balancer.ipdl4; path=/; domain=.wipo.int; JSES	N/A	Unknown	2009-11-16 21:27:49

Networkminor

By sajad hasan ali

NetworkMiner Analysis:

- **HTTP Cookie Parameter Protocol:**

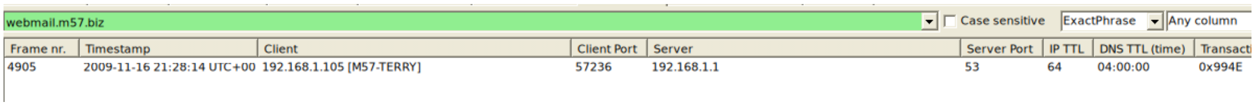
    - An **HTTP Cookie protocol** communication was identified between the device **192.168.1.105** (assigned to an employee identified as **m57-terry**) and the server **208.97.187.139** (webmail.m57.biz).

    - The **transmitted data** included a **deleted username** and the exposed password: `dEBpXAM5IKn2`.

    - **Credential Exposure:** The leaked password linked to **m57-terry** indicates a likely **internal security breach** or **unauthorized access to the employee's account**.

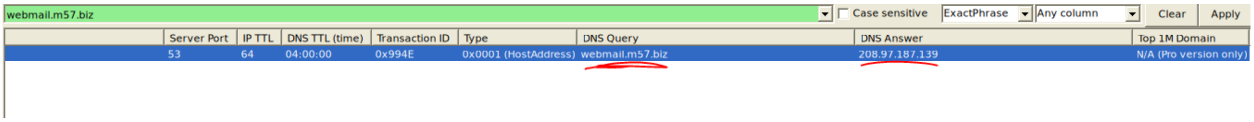
- **Recommended Response:** All **employees** must be required to **immediately change their passwords**, as this incident suggests that other credentials in the system may also be compromised.

DNS Analysis:



webmail.m57.biz ☐ Case sensitive ExactPhrase Any column

Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transacti
4905	2009-11-16 21:28:14 UTC+00	192.168.1.105 [M57-TERRY]	57236	192.168.1.1	53	64	04:00:00	0x994E



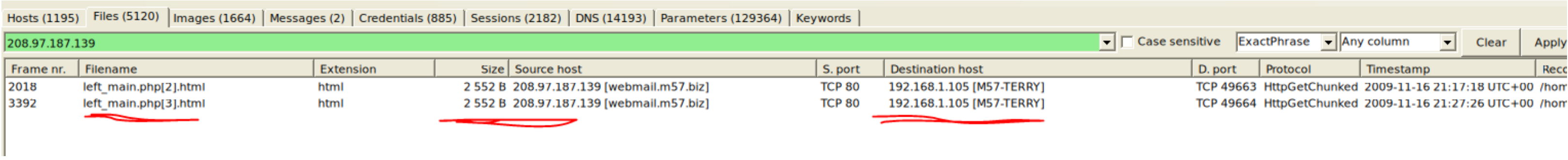
webmail.m57.biz ☐ Case sensitive ExactPhrase Any column Clear Apply

	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer	Top 1M Domain
	53	64	04:00:00	0x994E	0x0001 (HostAddress)	webmail.m57.biz	208.97.187.139	N/A (Pro version only)

Following the investigation, a **DNS lookup** was performed for the domain **webmail.m57.biz**. The result revealed that **webmail.m57.biz is not associated with the company’s official infrastructure**, but rather resolves to an **external IP address (208.97.187.139)**.

- This strongly suggests a **malicious attack involving an unauthorized external server**.

By sajad hasan ali



208.97.187.139 □ Case sensitive ExactPhrase Any column

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reco
2018	left_main.php[2].html	html	2 552 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49663	HttpGetChunked	2009-11-16 21:17:18 UTC+00	/hom
3392	left_main.php[3].html	html	2 552 B	208.97.187.139 [webmail.m57.biz]	TCP 80	192.168.1.105 [M57-TERRY]	TCP 49664	HttpGetChunked	2009-11-16 21:27:26 UTC+00	/hom

A **suspicious connection** was detected between the internal device (**192.168.1.105**, assigned to employee **m57-terry**) and an **external server** (**208.97.187.139**) over the **HTTP protocol**. During this connection, several **HTML files** with suspicious names such as `left_main.php[2].html` and `left_main.php[3].html` (each with a size of **2,552 bytes**) were downloaded.

These files may potentially contain **malicious code** or be part of an attempt to **compromise the internal device**.

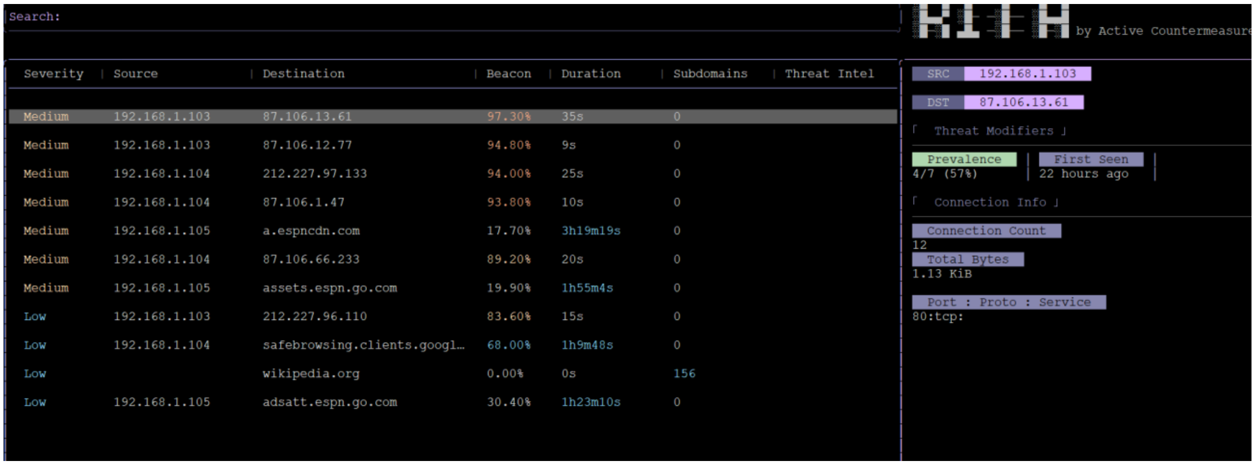
The files were downloaded from **webmail.m57.biz**, an **external server**, to the employee's machine. Since the HTML files were transmitted over **TCP port 80**, this suggests a possible **internal attack** or **exploitation of existing vulnerabilities**.

Recommendations and Actions:

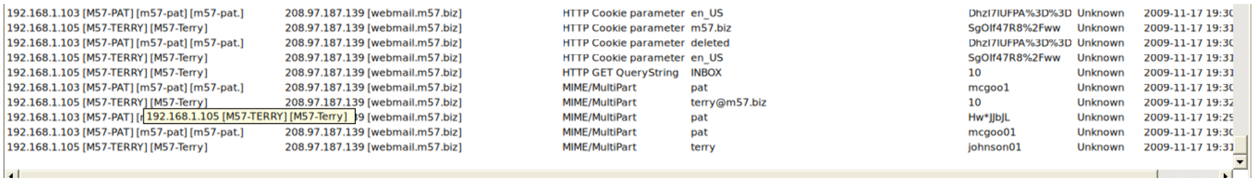
1. **Isolate device 192.168.1.50** from the network to allow deeper investigation of suspicious activities.
2. **Force a system-wide password reset** for all users to prevent further compromise of sensitive information.
3. **Monitor network activity closely** to detect any additional suspicious behaviors or data leaks.
4. **Conduct further analysis** of the suspicious connections and involved external servers to determine the full scope of the attack.

By sajad hasan ali

net-2009-11-17-10-32



```
Search:                                                                      RITA by Active Countermeasure

 Severity | Source          | Destination                 | Beacon | Duration  | Subdomains | Threat Intel     SRC  192.168.1.103

 Medium     192.168.1.103     87.106.13.61                  97.30%   35s         0                             DST  87.106.13.61
 Medium     192.168.1.103     87.106.12.77                  94.80%   9s          0                             Threat Modifiers
 Medium     192.168.1.104     212.227.97.133                94.00%   25s         0                             Prevalence  | First Seen
 Medium     192.168.1.104     87.106.1.47                   93.80%   10s         0                             4/7 (57%)   | 22 hours ago
 Medium     192.168.1.105     a.espncdn.com                 17.70%   3h19m19s    0                             Connection Info
 Medium     192.168.1.104     87.106.66.233                 89.20%   20s         0                             Connection Count
 Medium     192.168.1.105     assets.espn.go.com            19.90%   1h55m4s     0                             12
 Low        192.168.1.103     212.227.96.110                83.60%   15s         0                             Total Bytes
 Low        192.168.1.104     safebrowsing.clients.googl…   68.00%   1h9m48s     0                             1.13 KiB
 Low                          wikipedia.org                 0.00%    0s          156
 Low        192.168.1.105     adsatt.espn.go.com            30.40%   1h23m10s    0                             Port : Proto : Service
                                                                                                               80:tcp:
```



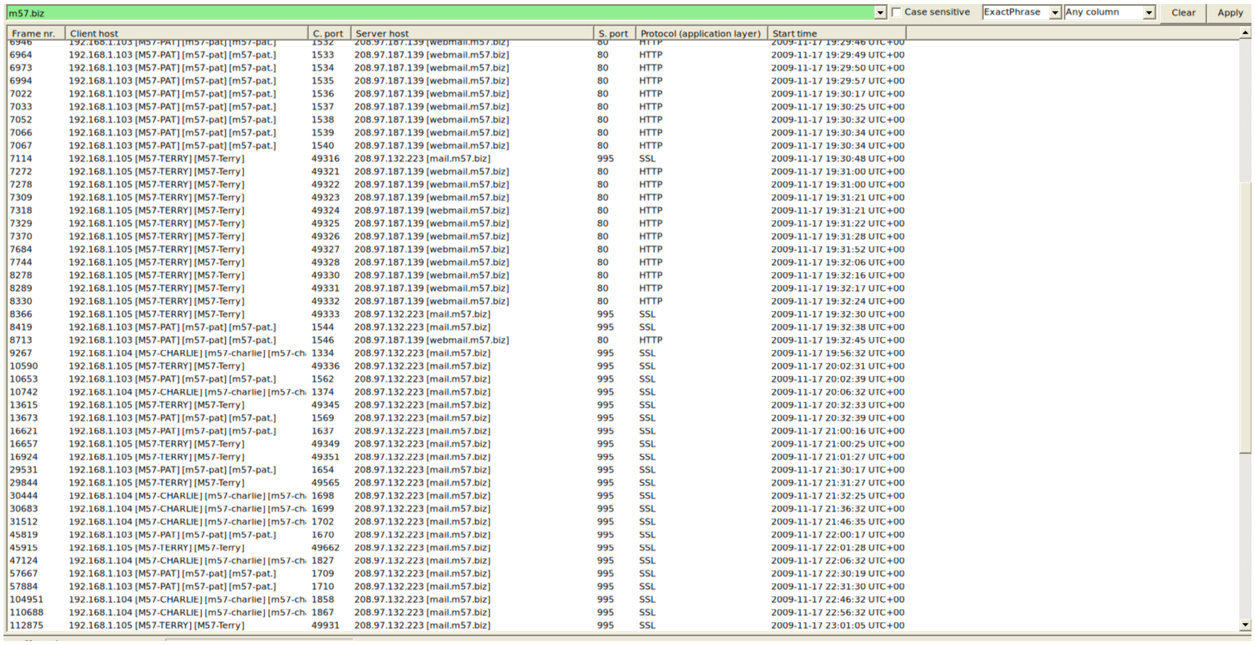
```
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]      208.97.187.139 [webmail.m57.biz]   HTTP Cookie parameter  en_US            DhzI7IUFPA%3D%3D  Unknown  2009-11-17 19:30
192.168.1.105 [M57-TERRY] [M57-Terry]             208.97.187.139 [webmail.m57.biz]   HTTP Cookie parameter  m57.biz          SgOIf47R8%2Fww    Unknown  2009-11-17 19:31
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]      208.97.187.139 [webmail.m57.biz]   HTTP Cookie parameter  deleted          DhzI7IUFPA%3D%3D  Unknown  2009-11-17 19:30
192.168.1.105 [M57-TERRY] [M57-Terry]             208.97.187.139 [webmail.m57.biz]   HTTP Cookie parameter  en_US            SgOIf47R8%2Fww    Unknown  2009-11-17 19:31
192.168.1.105 [M57-TERRY] [M57-Terry]             208.97.187.139 [webmail.m57.biz]   HTTP GET QueryString   INBOX            10                Unknown  2009-11-17 19:31
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]      208.97.187.139 [webmail.m57.biz]   MIME/MultiPart         pat              mcgoo1            Unknown  2009-11-17 19:30
192.168.1.105 [M57-TERRY] [M57-Terry]             208.97.187.139 [webmail.m57.biz]   MIME/MultiPart         terry@m57.biz    10                Unknown  2009-11-17 19:32
192.168.1.103 [M57-PAT] [192.168.1.105 [M57-TERRY] [M57-Terry]9 [webmail.m57.biz]    MIME/MultiPart         pat              Hw*JJbJL          Unknown  2009-11-17 19:29
192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]      208.97.187.139 [webmail.m57.biz]   MIME/MultiPart         pat              mcgoo01           Unknown  2009-11-17 19:30
192.168.1.105 [M57-TERRY] [M57-Terry]             208.97.187.139 [webmail.m57.biz]   MIME/MultiPart         terry            johnson01         Unknown  2009-11-17 19:31
```

Usernames such as **terry**, **pat**, and **johnson01** were exposed, and their associated passwords were discovered.

Some of the exposed passwords include:

- **terry@m57.biz**: Password is **Hw*JjBL**.
- **pat@m57.biz**: Password is **mcgoo01**.
- **johnson01**: Password is **Hw*JjBL**.

By sajad hasan ali



m57.biz ☐ Case sensitive ExactPhrase Any column

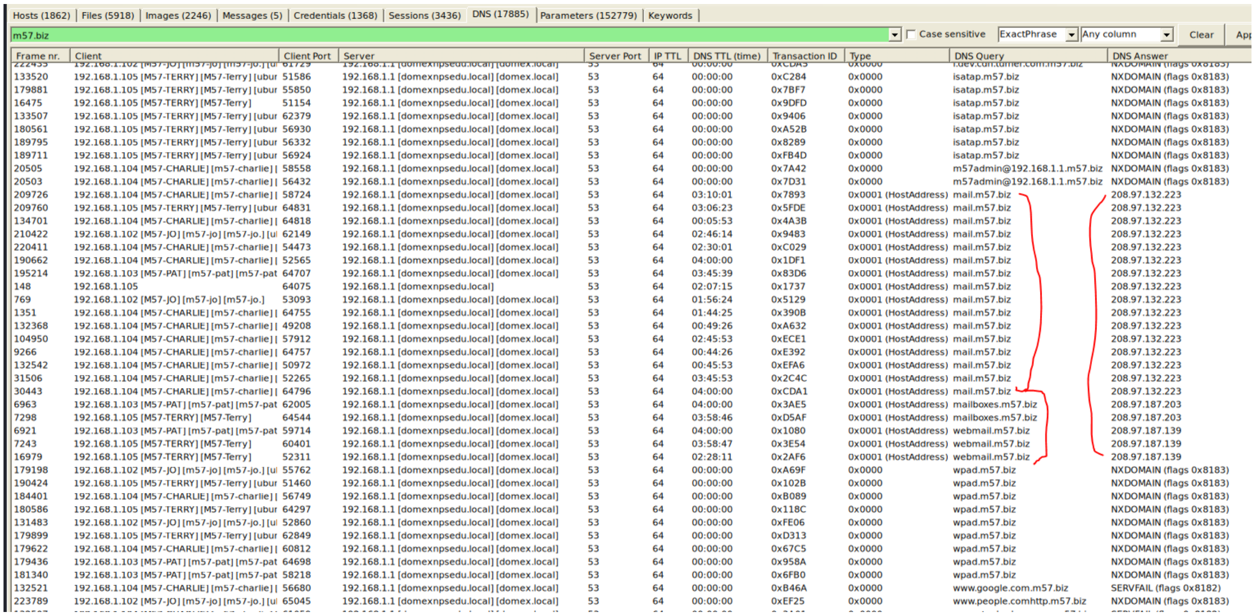
Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
6946	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1532	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:29:46 UTC+00
6964	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1533	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:29:49 UTC+00
6973	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1534	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:29:50 UTC+00
6994	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1535	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:29:57 UTC+00
7022	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1536	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:30:17 UTC+00
7033	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1537	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:30:25 UTC+00
7052	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1538	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:30:32 UTC+00
7066	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1539	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:30:34 UTC+00
7067	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1540	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:30:34 UTC+00
7114	192.168.1.105 [M57-TERRY] [M57-Terry]	49316	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 19:30:48 UTC+00
7272	192.168.1.105 [M57-TERRY] [M57-Terry]	49321	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:00 UTC+00
7278	192.168.1.105 [M57-TERRY] [M57-Terry]	49322	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:00 UTC+00
7309	192.168.1.105 [M57-TERRY] [M57-Terry]	49323	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:21 UTC+00
7318	192.168.1.105 [M57-TERRY] [M57-Terry]	49324	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:21 UTC+00
7329	192.168.1.105 [M57-TERRY] [M57-Terry]	49325	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:22 UTC+00
7370	192.168.1.105 [M57-TERRY] [M57-Terry]	49326	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:28 UTC+00
7684	192.168.1.105 [M57-TERRY] [M57-Terry]	49327	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:31:52 UTC+00
7744	192.168.1.105 [M57-TERRY] [M57-Terry]	49328	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:32:06 UTC+00
8278	192.168.1.105 [M57-TERRY] [M57-Terry]	49330	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:32:16 UTC+00
8289	192.168.1.105 [M57-TERRY] [M57-Terry]	49331	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:32:17 UTC+00
8330	192.168.1.105 [M57-TERRY] [M57-Terry]	49332	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:32:24 UTC+00
8366	192.168.1.105 [M57-TERRY] [M57-Terry]	49333	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 19:32:30 UTC+00
8419	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1544	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 19:32:38 UTC+00
8713	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1546	208.97.187.139 [webmail.m57.biz]	80	HTTP	2009-11-17 19:32:45 UTC+00
9267	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1334	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 19:56:32 UTC+00
10590	192.168.1.105 [M57-TERRY] [M57-Terry]	49336	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 20:02:31 UTC+00
10653	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1562	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 20:02:39 UTC+00
10742	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1374	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 20:06:32 UTC+00
13615	192.168.1.105 [M57-TERRY] [M57-Terry]	49345	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 20:32:33 UTC+00
13673	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1569	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 20:32:39 UTC+00
16621	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1637	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:00:16 UTC+00
16657	192.168.1.105 [M57-TERRY] [M57-Terry]	49349	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:00:25 UTC+00
16924	192.168.1.105 [M57-TERRY] [M57-Terry]	49351	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:01:27 UTC+00
29531	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1654	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:30:17 UTC+00
29844	192.168.1.105 [M57-TERRY] [M57-Terry]	49565	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:31:27 UTC+00
30444	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1698	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:32:25 UTC+00
30683	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1699	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:36:32 UTC+00
31512	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1702	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 21:46:35 UTC+00
45819	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1670	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:00:17 UTC+00
45915	192.168.1.105 [M57-TERRY] [M57-Terry]	49662	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:01:28 UTC+00
47124	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1827	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:06:32 UTC+00
57667	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1709	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:30:19 UTC+00
57884	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.]	1710	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:31:30 UTC+00
104951	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1858	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:46:32 UTC+00
110688	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	1867	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 22:56:32 UTC+00
112875	192.168.1.105 [M57-TERRY] [M57-Terry]	49931	208.97.132.223 [mail.m57.biz]	995	SSL	2009-11-17 23:01:05 UTC+00

Repeated Activity over HTTP and SSL:

Multiple sessions were observed between internal devices like **192.168.1.103** and **192.168.1.105**, and external servers such as **webmail.m57.biz** and **mailboxes.m57.biz** over **HTTP (Port 80)** and **SSL (Port 995)**.

- **Session Timing:**
  - **HTTP sessions** occur frequently with very short durations (just a few seconds).
  - **SSL sessions** last longer, indicating the exchange of encrypted data or more complex operations.
- **Involved Devices:**
  - **192.168.1.103** (**employee m57-pat**) and **192.168.1.105** (**employee m57-terry**) are actively involved, with continuous interaction between internal devices and suspicious servers.

Conclusion: The ongoing interactions with external servers via **SSL** and **HTTP** suggest a potential **persistent attack** or **data exfiltration**. The use of **SSL** makes it harder to monitor the transmitted data, increasing the likelihood that **sensitive information** is being sent to untrusted servers.



Hosts (1862) | Files (5918) | Images (2246) | Messages (5) | Credentials (1368) | Sessions (3436) | DNS (17885) | Parameters (152779) | Keywords

m57.biz ☐ Case sensitive ExactPhrase Any column Clear App

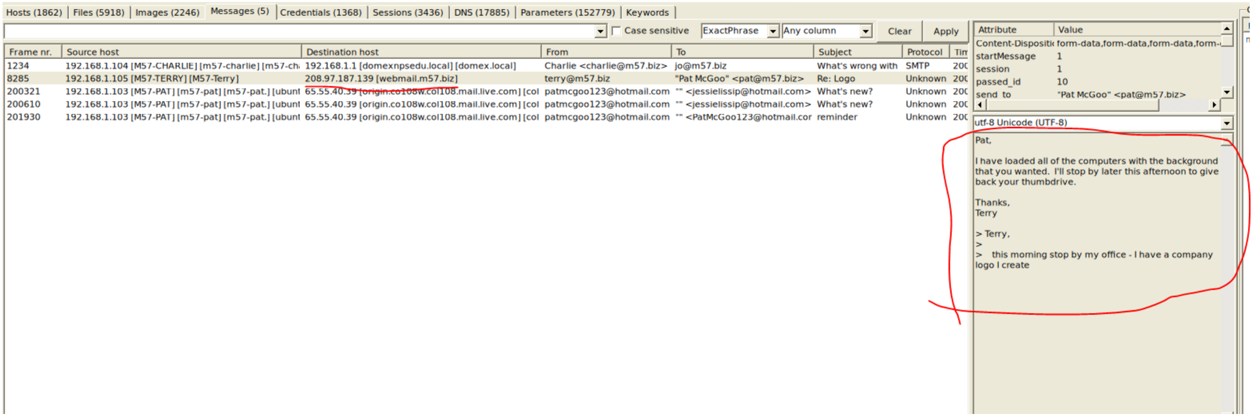
Frame nr.	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer
222433	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ul	61729	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xCDA3	0x0000	r.dev.cdn.turner.com.m57.biz	NXDOMAIN (flags 0x8183)
133520	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	51586	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xC284	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
179881	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	55850	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x7BF7	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
16475	192.168.1.105 [M57-TERRY] [M57-Terry]	51154	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x9DFD	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
133507	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	62379	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x9406	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
180561	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	56930	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xA52B	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
189795	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	56332	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x8289	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
189711	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	56924	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xFB4D	0x0000	isatap.m57.biz	NXDOMAIN (flags 0x8183)
20505	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	58558	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x7A42	0x0000	m57admin@192.168.1.1.m57.biz	NXDOMAIN (flags 0x8183)
20503	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	56432	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x7D31	0x0000	m57admin@192.168.1.1.m57.biz	NXDOMAIN (flags 0x8183)
209726	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	58724	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:10:01	0x7893	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
209760	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	64831	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:06:23	0x5FDE	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
134701	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	64818	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:05:53	0x4A3B	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
210422	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ul	62149	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:46:14	0x9483	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
220411	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	54473	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:30:01	0xC029	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
190662	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	52565	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	04:00:00	0x1DF1	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
195214	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat	64707	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:45:39	0x83D6	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
148	192.168.1.105	64075	192.168.1.1 [domexnpsedu.local]	53	64	02:07:15	0x1737	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
769	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.]	53093	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:56:24	0x5129	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
1351	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	64755	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	01:44:25	0x390B	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
132368	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	49208	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:49:26	0xA632	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
104950	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	57912	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:45:53	0xECE1	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
9266	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	64757	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:44:26	0xE392	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
132542	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	50972	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:45:53	0xEFA6	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
31506	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	52265	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:45:53	0x2C4C	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
30443	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	64796	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	04:00:00	0xCDA1	0x0001 (HostAddress)	mail.m57.biz	208.97.132.223
6963	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat	62005	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	04:00:00	0x3AE5	0x0001 (HostAddress)	mailboxes.m57.biz	208.97.187.203
7298	192.168.1.105 [M57-TERRY] [M57-Terry]	64544	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:58:46	0xD5AF	0x0001 (HostAddress)	mailboxes.m57.biz	208.97.187.203
6921	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat	59714	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	04:00:00	0x1080	0x0001 (HostAddress)	webmail.m57.biz	208.97.187.139
7243	192.168.1.105 [M57-TERRY] [M57-Terry]	60401	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	03:58:47	0x3E54	0x0001 (HostAddress)	webmail.m57.biz	208.97.187.139
16979	192.168.1.105 [M57-TERRY] [M57-Terry]	52311	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	02:28:11	0x2AF6	0x0001 (HostAddress)	webmail.m57.biz	208.97.187.139
179198	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ul	55762	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xA69F	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
190424	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	51460	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x102B	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
184401	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	56749	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xB089	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
180586	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	64297	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x118C	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
131483	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ul	52860	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xFE06	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
179899	192.168.1.105 [M57-TERRY] [M57-Terry] [ubur	62849	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xD313	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
179622	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	60812	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x67C5	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
179436	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat	64698	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x958A	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
181340	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat	58218	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0x6FB0	0x0000	wpad.m57.biz	NXDOMAIN (flags 0x8183)
132521	192.168.1.104 [M57-CHARLIE] [m57-charlie] [	56680	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xB46A	0x0000	www.google.com.m57.biz	SERVFAIL (flags 0x8182)
223789	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ul	65045	192.168.1.1 [domexnpsedu.local] [domex.local]	53	64	00:00:00	0xEF25	0x0000	www.people.comhttp.m57.biz	NXDOMAIN (flags 0x8183)

Suspicious **DNS queries** were detected to untrusted domains such as **mail.m57.biz** and **webmail.m57.biz**.

The presence of **NXDOMAIN** responses suggests attempts to access non-existent servers, which could indicate an **attack** or **data leakage**.

Recommended Actions:

1. Monitor **DNS queries** to suspicious domains.
2. Isolate suspicious domains (e.g., **m57.biz**) from the network.
3. Review affected devices and verify they have not been compromised.



Hosts (1862) | Files (5918) | Images (2246) | Messages (5) | Credentials (1368) | Sessions (3436) | DNS (17885) | Parameters (152779) | Keywords

☐ Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Tim
1234	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-ch	192.168.1.1 [domexnpsedu.local] [domex.local]	Charlie <charlie@m57.biz>	jo@m57.biz	What's wrong with	SMTP	20(
8285	192.168.1.105 [M57-TERRY] [M57-Terry]	208.97.187.139 [webmail.m57.biz]	terry@m57.biz	"Pat McGoo" <pat@m57.biz>	Re: Logo	Unknown	20(
200321	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.] [ubunt	65.55.40.39 [origin.co108w.col108.mail.live.com] [col	patmcgoo123@hotmail.com	"" <jessielissip@hotmail.com>	What's new?	Unknown	20(
200610	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.] [ubunt	65.55.40.39 [origin.co108w.col108.mail.live.com] [col	patmcgoo123@hotmail.com	"" <jessielissip@hotmail.com>	What's new?	Unknown	20(
201930	192.168.1.103 [M57-PAT] [m57-pat] [m57-pat.] [ubunt	65.55.40.39 [origin.co108w.col108.mail.live.com] [col	patmcgoo123@hotmail.com	"" <PatMcGoo123@hotmail.cor	reminder	Unknown	20(

Attribute	Value
Content-Dispositi	form-data,form-data,form-data,form-(
startMessage	1
session	1
passed_id	10
send_to	"Pat McGoo" <pat@m57.biz>

utf-8 Unicode (UTF-8)

```
Pat,

I have loaded all of the computers with the background
that you wanted.  I'll stop by later this afternoon to give
back your thumbdrive.

Thanks,
Terry

> Terry,
>
>    this morning stop by my office - I have a company
logo I create
```

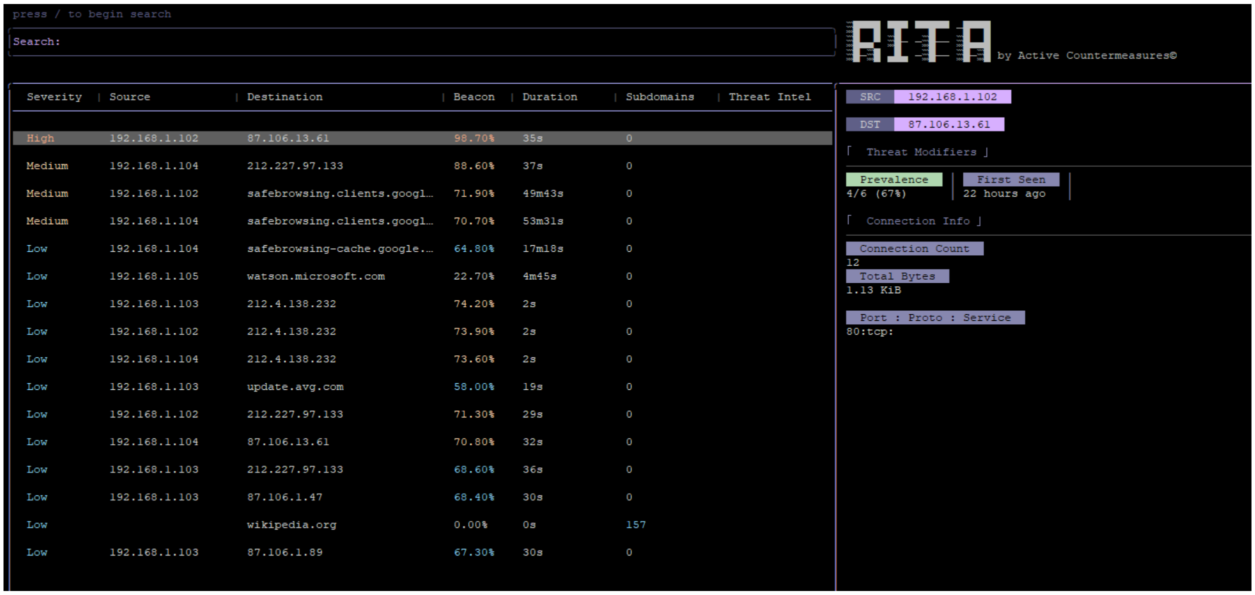
- **Source Host: 192.168.1.105** (device **m57-pat**) communicated with **external server 208.97.187.139**, which resolves to **webmail.m57.biz.**

By sajad hasan ali

- **Protocols Involved:** The communication used **unknown** protocols, indicating suspicious activity.

- **Email Content:** The email from **m57-pat** to **Pat McGoo** includes an informal message about loading files onto computers as requested, with a plan to meet later in the day. It also mentions a suspicious company logo, which may be part of a **malware distribution** or **phishing** attempt.

net-2009-11-18-10-32

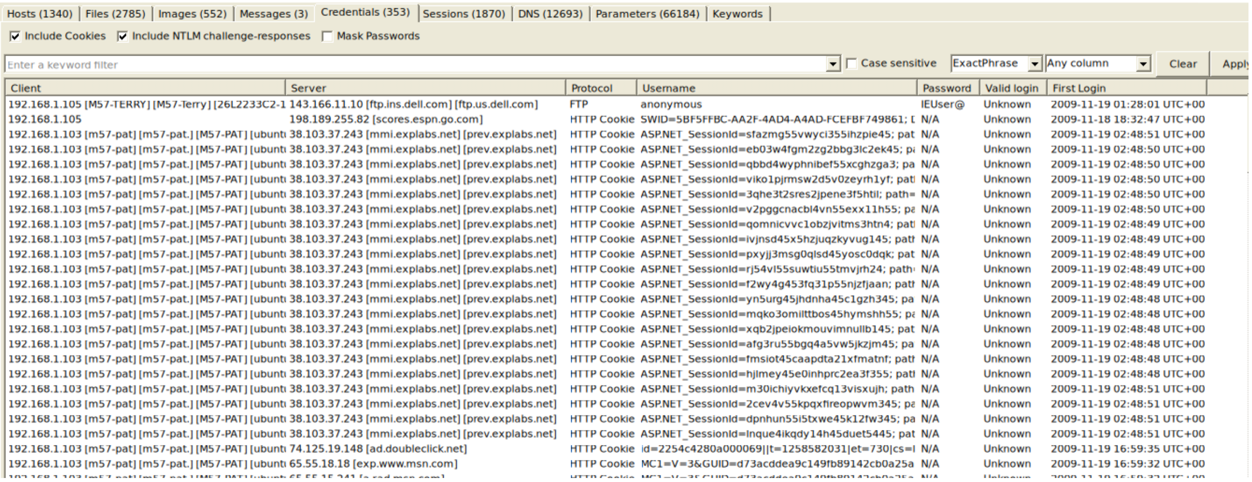


```
press / to begin search
Search:

 Severity | Source          | Destination                  | Beacon | Duration  | Subdomains | Threat Intel     SRC  192.168.1.102

 High      192.168.1.102    87.106.13.61                   98.70%   35s         0                              DST  87.106.13.61

 Medium    192.168.1.104    212.227.97.133                 88.60%   37s         0                              ⌈  Threat Modifiers ⌋

 Medium    192.168.1.102    safebrowsing.clients.googl…    71.90%   49m43s      0                              Prevalence  | First Seen   |
                                                                                                               4/6 (67%)   | 22 hours ago |
 Medium    192.168.1.104    safebrowsing.clients.googl…    70.70%   53m31s      0
                                                                                                               ⌈  Connection Info ⌋
 Low       192.168.1.104    safebrowsing-cache.google.…    64.80%   17m18s      0
                                                                                                               Connection Count
 Low       192.168.1.105    watson.microsoft.com           22.70%   4m45s       0                              12
                                                                                                               Total Bytes
 Low       192.168.1.103    212.4.138.232                  74.20%   2s          0                              1.13 KiB

 Low       192.168.1.102    212.4.138.232                  73.90%   2s          0                              Port : Proto : Service
                                                                                                               80:tcp:
 Low       192.168.1.104    212.4.138.232                  73.60%   2s          0

 Low       192.168.1.103    update.avg.com                 58.00%   19s         0

 Low       192.168.1.102    212.227.97.133                 71.30%   29s         0

 Low       192.168.1.104    87.106.13.61                   70.80%   32s         0

 Low       192.168.1.103    212.227.97.133                 68.60%   36s         0

 Low       192.168.1.103    87.106.1.47                    68.40%   30s         0

 Low                        wikipedia.org                  0.00%    0s          157

 Low       192.168.1.103    87.106.1.89                    67.30%   30s         0
```

A high-risk connection was detected between **192.168.1.102** and **87.106.13.61**, with a **98.70% repetition rate** over a **35-second duration**.

This activity suggests ongoing communication with an external server, potentially indicating a **persistent attack** or **data exfiltration**.

By sajad hasan ali



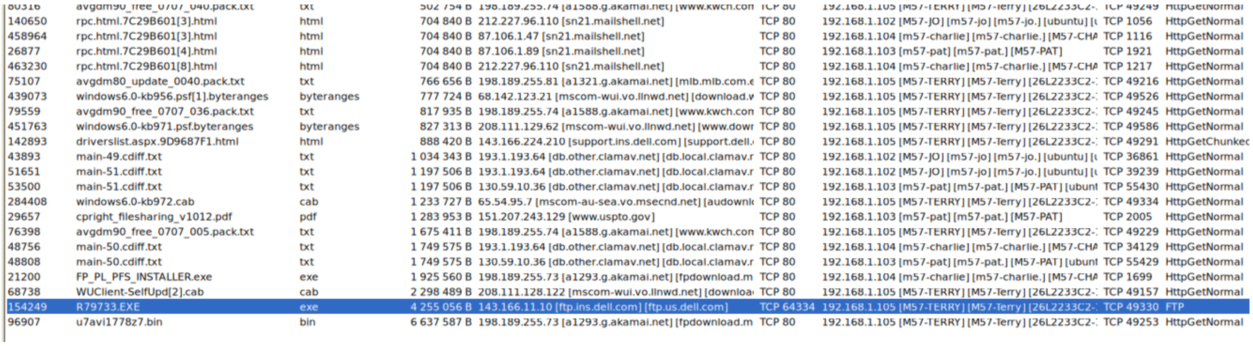
Hosts (1340) | Files (2785) | Images (552) | Messages (3) | Credentials (353) | Sessions (1870) | DNS (12693) | Parameters (66184) | Keywords

☑ Include Cookies ☑ Include NTLM challenge-responses □ Mask Passwords

Enter a keyword filter □ Case sensitive ExactPhrase Any column Clear Apply

Client	Server	Protocol	Username	Password	Valid login	First Login
192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-1	143.166.11.10 [ftp.ins.dell.com] [ftp.us.dell.com]	FTP	anonymous	IEUser@	Unknown	2009-11-19 01:28:01 UTC+00
192.168.1.105	198.189.255.82 [scores.espn.go.com]	HTTP Cookie	SWID=5BF5FFBC-AA2F-4AD4-A4AD-FCEFBF749861; [	N/A	Unknown	2009-11-18 18:32:47 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=sfazmg55vwyci355ihzpie45; pat	N/A	Unknown	2009-11-19 02:48:51 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=eb03w4fgm2zg2bbg3lc2ek45; pa	N/A	Unknown	2009-11-19 02:48:50 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=qbbd4wyphnibef55xcghzga3; pa	N/A	Unknown	2009-11-19 02:48:50 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=viko1pjrmsw2d5v0zeyrh1yf; pat	N/A	Unknown	2009-11-19 02:48:50 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=3qhe3t2sres2jpene3f5htil; path=	N/A	Unknown	2009-11-19 02:48:50 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=v2pggcnacbl4vn55exx11h55; pa	N/A	Unknown	2009-11-19 02:48:50 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=qomnicvvc1obzjvitms3htn4; pat	N/A	Unknown	2009-11-19 02:48:49 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=ivjnsd45x5hzjuqzkyvug145; path	N/A	Unknown	2009-11-19 02:48:49 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=pxyjj3msg0qlsd45yosc0dqk; pat	N/A	Unknown	2009-11-19 02:48:49 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=rj54vl55suwtiu55tmvjrh24; path	N/A	Unknown	2009-11-19 02:48:49 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=f2wy4g453fq31p55njzfjaan; path	N/A	Unknown	2009-11-19 02:48:49 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=yn5urg45jhdnha45c1gzh345; pa	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=mqko3omilttbos45hymshh55; pa	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=xqb2jpeiokmouvimnullb145; pat	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=afg3ru55bgq4a5vw5jkzjm45; pa	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=fmsiot45caapdta21xfmatnf; path	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=hjlmey45e0inhprc2ea3f355; path	N/A	Unknown	2009-11-19 02:48:48 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=m30ichiyvkxefcq13visxujh; path	N/A	Unknown	2009-11-19 02:48:51 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=2cev4v55kpqxfireopwvm345; pa	N/A	Unknown	2009-11-19 02:48:51 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=dpnhun55i5txwe45k12fw345; pa	N/A	Unknown	2009-11-19 02:48:51 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=lnque4ikqdy14h45duet5445; pat	N/A	Unknown	2009-11-19 02:48:51 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	74.125.19.148 [ad.doubleclick.net]	HTTP Cookie	id=2254c4280a000069||t=1258582031|et=730|cs=I	N/A	Unknown	2009-11-19 16:59:35 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	65.55.18.18 [exp.www.msn.com]	HTTP Cookie	MC1=V=3&GUID=d73acddea9c149fb89142cb0a25a	N/A	Unknown	2009-11-19 16:59:32 UTC+00
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	65.55.15.241 [a.rad.msn.com]	HTTP Cookie	MC1=V=3&GUID=d73acddea9c149fb89142cb0a25a	N/A	Unknown	2009-11-19 16:59:32 UTC+00

An **FTP connection** was detected using the **anonymous** username, which exposes the system to potential risks.



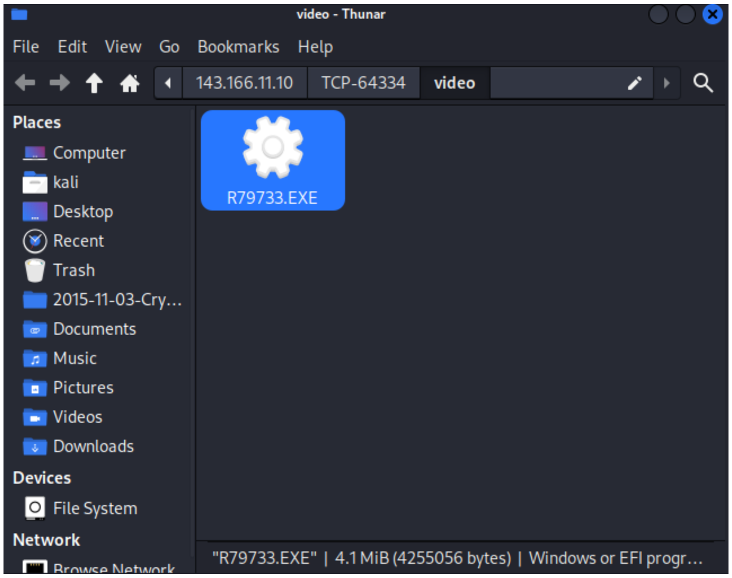
80316	avgdm90_free_0707_040.pack.txt	txt	502 754 B	198.189.255.74 [a1588.g.akamai.net] [www.kwch.con	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49249	HttpGetNormal
140650	rpc.html.7C29B601[3].html	html	704 840 B	212.227.96.110 [sn21.mailshell.net]	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ubuntu] [ι	TCP 1056	HttpGetNormal
458964	rpc.html.7C29B601[3].html	html	704 840 B	87.106.1.47 [sn21.mailshell.net]	TCP 80	192.168.1.104 [m57-charlie] [m57-charlie.] [M57-CHA	TCP 1116	HttpGetNormal
26877	rpc.html.7C29B601[4].html	html	704 840 B	87.106.1.89 [sn21.mailshell.net]	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT]	TCP 1921	HttpGetNormal
463230	rpc.html.7C29B601[8].html	html	704 840 B	212.227.96.110 [sn21.mailshell.net]	TCP 80	192.168.1.104 [m57-charlie] [m57-charlie.] [M57-CHA	TCP 1217	HttpGetNormal
75107	avgdm80_update_0040.pack.txt	txt	766 656 B	198.189.255.81 [a1321.g.akamai.net] [mlb.mlb.com.e	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49216	HttpGetNormal
439073	windows6.0-kb956.psf[1].byteranges	byteranges	777 724 B	68.142.123.21 [mscom-wui.vo.llnwd.net] [download.w	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49526	HttpGetNormal
79559	avgdm90_free_0707_036.pack.txt	txt	817 935 B	198.189.255.74 [a1588.g.akamai.net] [www.kwch.con	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49245	HttpGetNormal
451763	windows6.0-kb971.psf.byteranges	byteranges	827 313 B	208.111.129.62 [mscom-wui.vo.llnwd.net] [www.dowr	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49586	HttpGetNormal
142893	driverslist.aspx.9D9687F1.html	html	888 420 B	143.166.224.210 [support.ins.dell.com] [support.dell.	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49291	HttpGetChunked
43893	main-49.cdiff.txt	txt	1 034 343 B	193.1.193.64 [db.other.clamav.net] [db.local.clamav.r	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ubuntu] [ι	TCP 36861	HttpGetNormal
51651	main-51.cdiff.txt	txt	1 197 506 B	193.1.193.64 [db.other.clamav.net] [db.local.clamav.r	TCP 80	192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] [ubuntu] [ι	TCP 39239	HttpGetNormal
53500	main-51.cdiff.txt	txt	1 197 506 B	130.59.10.36 [db.other.clamav.net] [db.local.clamav.r	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	TCP 55430	HttpGetNormal
284408	windows6.0-kb972.cab	cab	1 233 727 B	65.54.95.7 [mscom-au-sea.vo.msecnd.net] [audownl	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49334	HttpGetNormal
29657	cpright_filesharing_v1012.pdf	pdf	1 283 953 B	151.207.243.129 [www.uspto.gov]	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT]	TCP 2005	HttpGetNormal
76398	avgdm90_free_0707_005.pack.txt	txt	1 675 411 B	198.189.255.74 [a1588.g.akamai.net] [www.kwch.con	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49229	HttpGetNormal
48756	main-50.cdiff.txt	txt	1 749 575 B	193.1.193.64 [db.other.clamav.net] [db.local.clamav.r	TCP 80	192.168.1.104 [m57-charlie] [m57-charlie.] [M57-CHA	TCP 34129	HttpGetNormal
48808	main-50.cdiff.txt	txt	1 749 575 B	130.59.10.36 [db.other.clamav.net] [db.local.clamav.r	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubunt	TCP 55429	HttpGetNormal
21200	FP_PL_PFS_INSTALLER.exe	exe	1 925 560 B	198.189.255.73 [a1293.g.akamai.net] [fpdownload.m	TCP 80	192.168.1.104 [m57-charlie] [m57-charlie.] [M57-CHA	TCP 1699	HttpGetNormal
68738	WUClient-SelfUpd[2].cab	cab	2 298 489 B	208.111.128.122 [mscom-wui.vo.llnwd.net] [downloa	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49157	HttpGetNormal
154249	R79733.EXE	exe	4 255 056 B	143.166.11.10 [ftp.ins.dell.com] [ftp.us.dell.com]	TCP 64334	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49330	FTP
96907	u7avi1778z7.bin	bin	6 637 587 B	198.189.255.73 [a1293.g.akamai.net] [fpdownload.m	TCP 80	192.168.1.105 [M57-TERRY] [M57-Terry] [26L2233C2-:	TCP 49253	HttpGetNormal

Large files were detected being sent via **HTTP** and **FTP** to suspicious servers such as **ftp.ins.dell.com** and **mscom-wu.io.msce.dns**.

The transferred files include **EXE** and **BIN** formats, which may contain **malicious code**.

By sajad hasan ali

The attached files



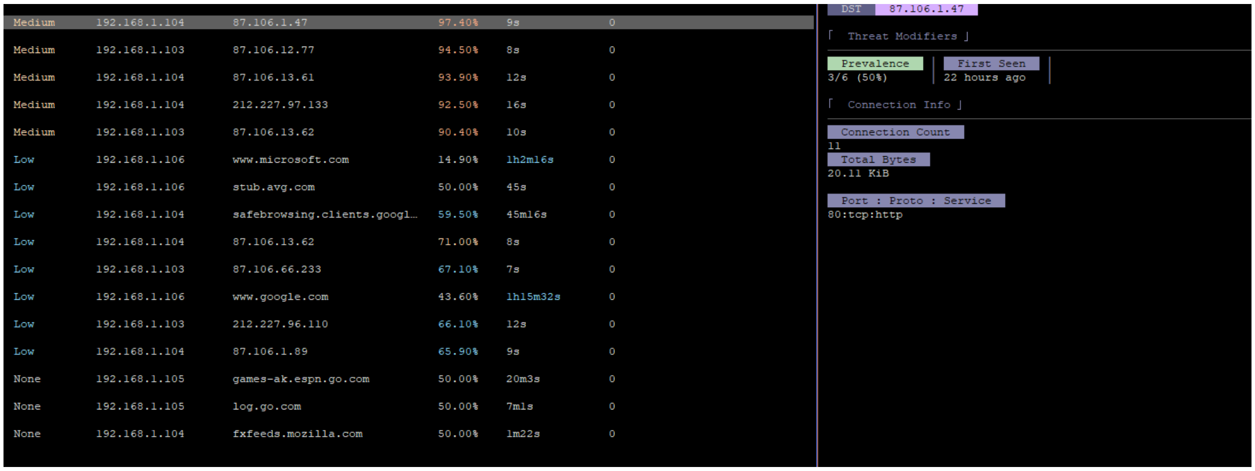
"R79733.EXE" | 4.1 MiB (4255056 bytes) | Windows or EFI progr…

Recommended Actions:

1. Review and examine the sent files to ensure they are safe.
2. Conduct a comprehensive security scan on all affected devices.
3. Immediately change passwords for all compromised accounts.
4. Isolate affected devices from the network if they contain malicious files.
5. Disable **FTP** protocols and switch to secure protocols like **SFTP**.

By sajad hasan ali

net-2009-11-20-10-30.pcap

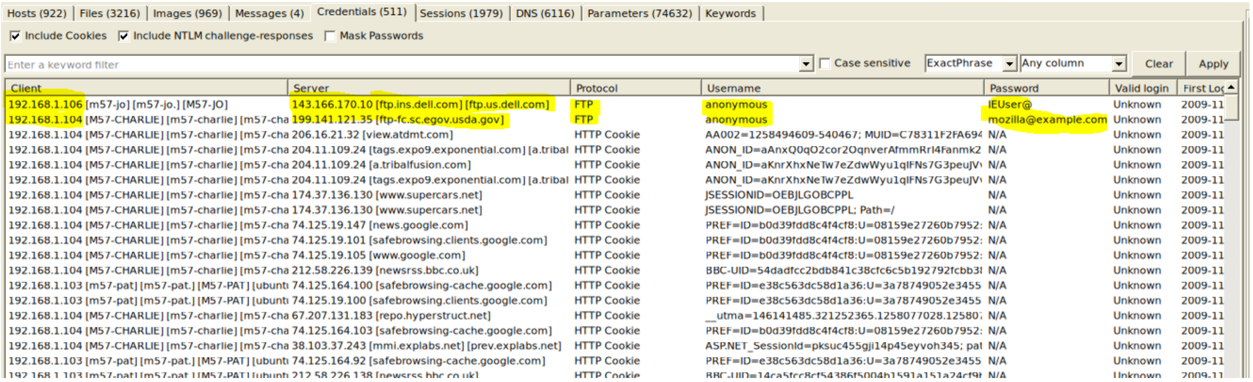


```
Medium    192.168.1.104    87.106.1.47                      97.40%    9s          0
Medium    192.168.1.103    87.106.12.77                     94.50%    8s          0
Medium    192.168.1.104    87.106.13.61                     93.90%    12s         0
Medium    192.168.1.104    212.227.97.133                   92.50%    16s         0
Medium    192.168.1.103    87.106.13.62                     90.40%    10s         0
Low       192.168.1.106    www.microsoft.com                14.90%    1h2m16s     0
Low       192.168.1.106    stub.avg.com                     50.00%    45s         0
Low       192.168.1.104    safebrowsing.clients.googl…      59.50%    45m16s      0
Low       192.168.1.104    87.106.13.62                     71.00%    8s          0
Low       192.168.1.103    87.106.66.233                    67.10%    7s          0
Low       192.168.1.106    www.google.com                   43.60%    1h15m32s    0
Low       192.168.1.103    212.227.96.110                   66.10%    12s         0
Low       192.168.1.104    87.106.1.89                      65.90%    9s          0
None      192.168.1.105    games-ak.espn.go.com             50.00%    20m3s       0
None      192.168.1.105    log.go.com                       50.00%    7m1s        0
None      192.168.1.104    fxfeeds.mozilla.com              50.00%    1m22s       0
```

```
DST  87.106.1.47

⌈ Threat Modifiers ⌋

Prevalence        | First Seen      |
3/6 (50%)         | 22 hours ago    |

⌈ Connection Info ⌋

Connection Count
11
Total Bytes
20.11 KiB

Port : Proto : Service
80:tcp:http
```

Medium-risk connections were detected between internal devices and suspicious servers.

The data transmitted was moderate in volume, using the **HTTP protocol**.

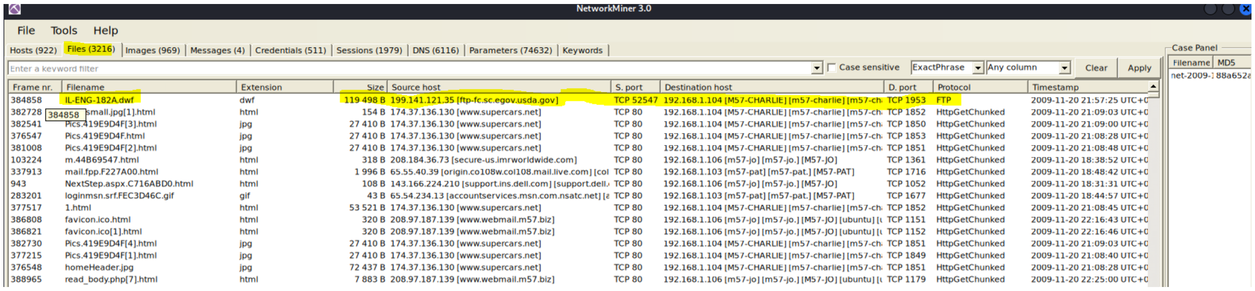


☑ Include Cookies ☑ Include NTLM challenge-responses ☐ Mask Passwords

☐ Case sensitive ExactPhrase Any column

Client	Server	Protocol	Username	Password	Valid login	First Log
192.168.1.106 [m57-jo] [m57-jo.] [M57-JO]	143.166.170.10 [ftp.ins.dell.com] [ftp.us.dell.com]	FTP	anonymous	IEUser@	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	199.141.121.35 [ftp-fc.sc.egov.usda.gov]	FTP	anonymous	mozilla@example.com	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	206.16.21.32 [view.atdmt.com]	HTTP Cookie	AA002=1258494609-540467; MUID=C78311F2FA694	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	204.11.109.24 [tags.expo9.exponential.com] [a.tribal	HTTP Cookie	ANON_ID=aAnxQ0qO2cor2OqnverAfmmRrl4Fanmk2	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	204.11.109.24 [a.tribalfusion.com]	HTTP Cookie	ANON_ID=aKnrXhxNeTw7eZdwWyu1qIFNs7G3peuJVı	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	204.11.109.24 [tags.expo9.exponential.com] [a.tribal	HTTP Cookie	ANON_ID=aKnrXhxNeTw7eZdwWyu1qIFNs7G3peuJVı	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	174.37.136.130 [www.supercars.net]	HTTP Cookie	JSESSIONID=OEBJLGOBCPPL	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	174.37.136.130 [www.supercars.net]	HTTP Cookie	JSESSIONID=OEBJLGOBCPPL; Path=/	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.19.147 [news.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.19.101 [safebrowsing.clients.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.19.105 [www.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	212.58.226.139 [newsrss.bbc.co.uk]	HTTP Cookie	BBC-UID=54dadfcc2bdb841c38cfc6c5b192792fcbb3ŧ	N/A	Unknown	2009-11
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubuntı	74.125.164.100 [safebrowsing-cache.google.com]	HTTP Cookie	PREF=ID=e38c563dc58d1a36:U=3a78749052e3455	N/A	Unknown	2009-11
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubuntı	74.125.19.100 [safebrowsing.clients.google.com]	HTTP Cookie	PREF=ID=e38c563dc58d1a36:U=3a78749052e3455	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	67.207.131.183 [repo.hyperstruct.net]	HTTP Cookie	__utma=146141485.321252365.1258077028.12580ī	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	74.125.164.103 [safebrowsing-cache.google.com]	HTTP Cookie	PREF=ID=b0d39fdd8c4f4cf8:U=08159e27260b7952:	N/A	Unknown	2009-11
192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-cha	38.103.37.243 [mmi.explabs.net] [prev.explabs.net]	HTTP Cookie	ASP.NET_SessionId=pksuc455gji14p45eyvoh345; pat	N/A	Unknown	2009-11
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubuntı	74.125.164.92 [safebrowsing-cache.google.com]	HTTP Cookie	PREF=ID=e38c563dc58d1a36:U=3a78749052e3455	N/A	Unknown	2009-11
192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT] [ubuntı	212.58.226.138 [newsrss.bbc.co.uk]	HTTP Cookie	BBC-UID=14ca5fcc8cf54386f5004b1591a151a24cf9ŧ	N/A	Unknown	2009-11

An **FTP connection** was detected using the **anonymous** username, which exposes the system to potential risks.



☐ Case sensitive ExactPhrase Any column

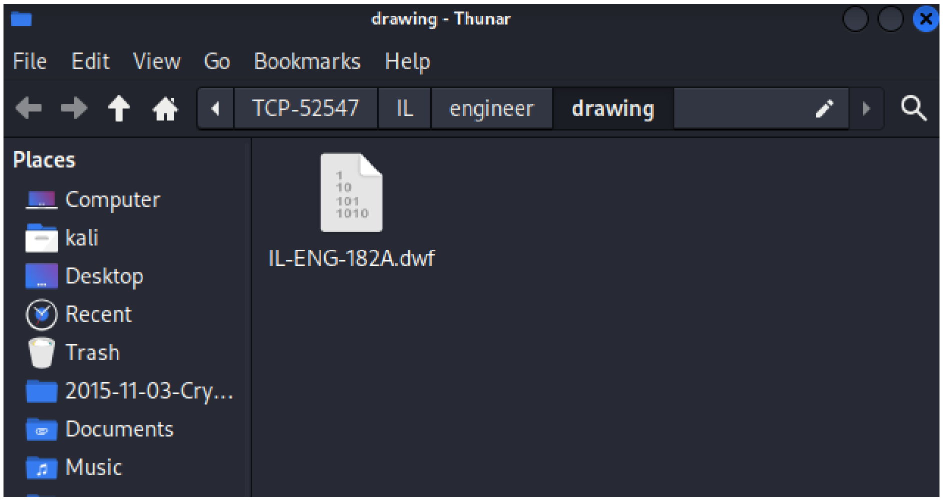
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
384858	IL-ENG-182A.dwf	dwf	119 498 B	199.141.121.35 [ftp-fc.sc.egov.usda.gov]	TCP 52547	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1953	FTP	2009-11-20 21:57:25 UTC+0
382728	small.jpg[1].html	html	154 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1852	HttpGetChunked	2009-11-20 21:09:03 UTC+0
382541	Pics.419E9D4F[3].html	jpg	27 410 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1850	HttpGetChunked	2009-11-20 21:09:00 UTC+0
376547	Pics.419E9D4F.html	jpg	27 410 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1853	HttpGetChunked	2009-11-20 21:08:28 UTC+0
381008	Pics.419E9D4F[2].html	jpg	27 410 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1851	HttpGetChunked	2009-11-20 21:08:48 UTC+0
103224	m.44B69547.html	html	318 B	208.184.36.73 [secure-us.imrworldwide.com]	TCP 80	192.168.1.106 [m57-jo] [m57-jo.] [M57-JO]	TCP 1361	HttpGetChunked	2009-11-20 18:38:52 UTC+0
337913	mail.fpp.F227A00.html	html	1 996 B	65.55.40.39 [origin.co108w.col108.mail.live.com] [col	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT]	TCP 1716	HttpGetChunked	2009-11-20 18:48:42 UTC+0
943	NextStep.aspx.C716ABD0.html	html	108 B	143.166.224.210 [support.ins.dell.com] [support.dell.	TCP 80	192.168.1.106 [m57-jo] [m57-jo.] [M57-JO]	TCP 1052	HttpGetChunked	2009-11-20 18:31:31 UTC+0
283201	loginmsn.srf.FEC3D46C.gif	gif	43 B	65.54.234.13 [accountservices.msn.com.nsatc.net] [a	TCP 80	192.168.1.103 [m57-pat] [m57-pat.] [M57-PAT]	TCP 1677	HttpGetChunked	2009-11-20 18:44:57 UTC+0
377517	1.html	html	53 521 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1852	HttpGetChunked	2009-11-20 21:08:45 UTC+0
386808	favicon.ico.html	html	320 B	208.97.187.139 [www.webmail.m57.biz]	TCP 80	192.168.1.106 [m57-jo] [m57-jo.] [M57-JO] [ubuntu] [u	TCP 1151	HttpGetChunked	2009-11-20 22:16:43 UTC+0
386821	favicon.ico[1].html	html	320 B	208.97.187.139 [www.webmail.m57.biz]	TCP 80	192.168.1.106 [m57-jo] [m57-jo.] [M57-JO] [ubuntu] [u	TCP 1152	HttpGetChunked	2009-11-20 22:16:46 UTC+0
382730	Pics.419E9D4F[4].html	jpg	27 410 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1851	HttpGetChunked	2009-11-20 21:09:03 UTC+0
377215	Pics.419E9D4F[1].html	jpg	27 410 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1849	HttpGetChunked	2009-11-20 21:08:40 UTC+0
376548	homeHeader.jpg	jpg	72 437 B	174.37.136.130 [www.supercars.net]	TCP 80	192.168.1.104 [M57-CHARLIE] [m57-charlie] [m57-chı	TCP 1851	HttpGetChunked	2009-11-20 21:08:28 UTC+0
388965	read_body.php[7].html	html	7 883 B	208.97.187.139 [www.webmail.m57.biz]	TCP 80	192.168.1.106 [m57-jo] [m57-jo.] [M57-JO] [ubuntu] [u	TCP 1179	HttpGetChunked	2009-11-20 22:25:00 UTC+0

Filename	MD5
net-2009-1	88a652a

Large files were detected being sent via **FTP**, including the file **IL-ENG-182.A.dwf**.

By sajad hasan ali

The attached files



IL-ENG-182A.dwf

By sajad hasan ali