Digital Forensics

2021SM_CS_6419_FRE1A

Assignment-02

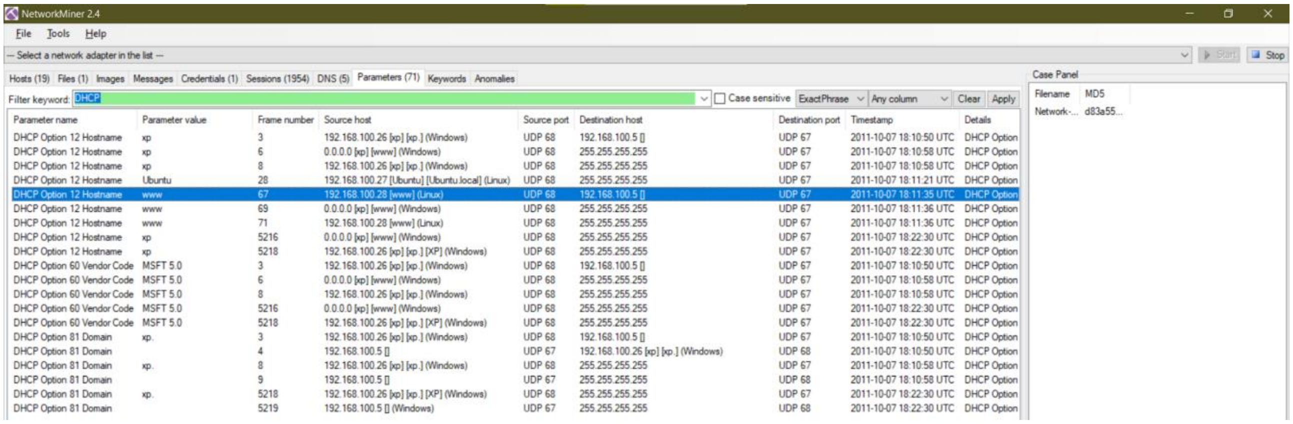
Prepared by:
Mohammadali Rahnama

Student number:
3709515

EST. 1785
UNB
UNIVERSITY OF NEW BRUNSWICK

1. What computer is serving as DHCP server? How do you know?

192.168.100.5 is the DHCP server, in the "Parameter" tab 192.168.100.5 is the Destination host.


NetworkMiner 2.4
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (19) Files (1) Images Messages Credentials (1) Sessions (1954) DNS (5) Parameters (71) Keywords Anomalies
Clear
Apply
Case Panel

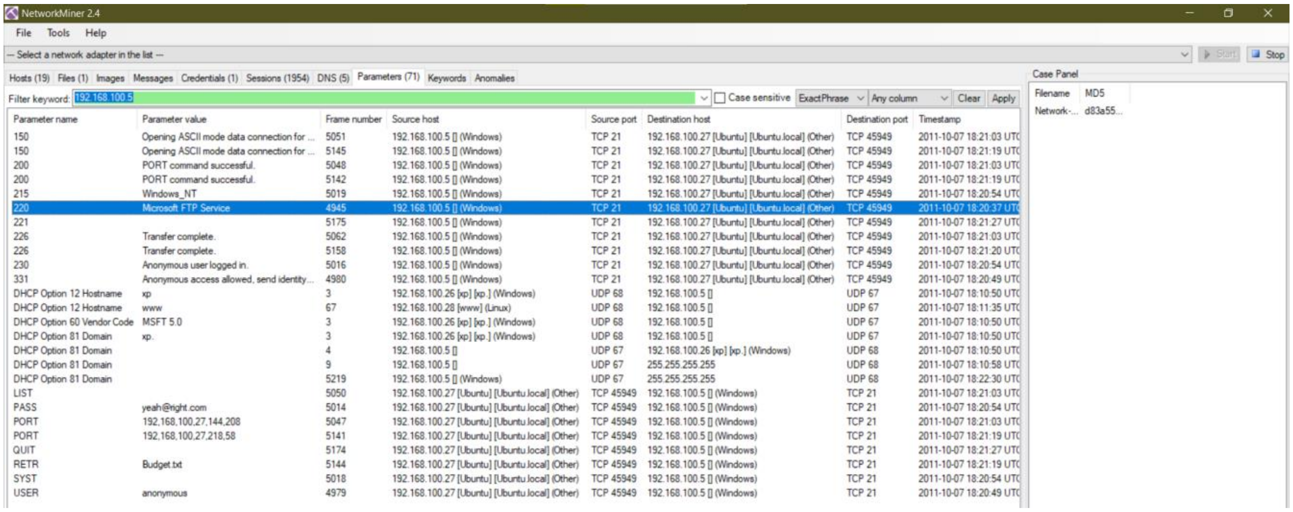
Filter keyword: DHCP
☐ Case sensitive ExactPhrase Any column

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Timestamp	Details
DHCP Option 12 Hostname	xp	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC	DHCP Option
DHCP Option 12 Hostname	xp	6	0.0.0.0 [xp] [www] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 12 Hostname	xp	8	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 12 Hostname	Ubuntu	28	192.168.100.27 [Ubuntu] [Ubuntu.local] (Linux)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:11:21 UTC	DHCP Option
DHCP Option 12 Hostname	www	67	192.168.100.28 [www] (Linux)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:11:35 UTC	DHCP Option
DHCP Option 12 Hostname	www	69	0.0.0.0 [xp] [www] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:11:36 UTC	DHCP Option
DHCP Option 12 Hostname	www	71	192.168.100.28 [www] (Linux)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:11:36 UTC	DHCP Option
DHCP Option 12 Hostname	xp	5216	0.0.0.0 [xp] [www] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:22:30 UTC	DHCP Option
DHCP Option 12 Hostname	xp	5218	192.168.100.26 [xp] [xp.] [XP] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:22:30 UTC	DHCP Option
DHCP Option 60 Vendor Code	MSFT 5.0	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC	DHCP Option
DHCP Option 60 Vendor Code	MSFT 5.0	6	0.0.0.0 [xp] [www] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 60 Vendor Code	MSFT 5.0	8	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 60 Vendor Code	MSFT 5.0	5216	0.0.0.0 [xp] [www] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:22:30 UTC	DHCP Option
DHCP Option 60 Vendor Code	MSFT 5.0	5218	192.168.100.26 [xp] [xp.] [XP] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:22:30 UTC	DHCP Option
DHCP Option 81 Domain	xp.	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC	DHCP Option
DHCP Option 81 Domain		4	192.168.100.5 []	UDP 67	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	2011-10-07 18:10:50 UTC	DHCP Option
DHCP Option 81 Domain	xp.	8	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 81 Domain		9	192.168.100.5 []	UDP 67	255.255.255.255	UDP 68	2011-10-07 18:10:58 UTC	DHCP Option
DHCP Option 81 Domain	xp.	5218	192.168.100.26 [xp] [xp.] [XP] (Windows)	UDP 68	255.255.255.255	UDP 67	2011-10-07 18:22:30 UTC	DHCP Option
DHCP Option 81 Domain		5219	192.168.100.5 [] (Windows)	UDP 67	255.255.255.255	UDP 68	2011-10-07 18:22:30 UTC	DHCP Option

Filename	MD5
Network-...	d83a55...

2. What other services is the DHCP server running? How do you know?

By adding the “192.168.100.5” filter keyword we can see that 192.168.100.5 is also running Microsoft FTP Service as well.


NetworkMiner 2.4
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (19) Files (1) Images Messages Credentials (1) Sessions (1954) DNS (5) Parameters (71) Keywords Anomalies
Clear
Apply
Case Panel

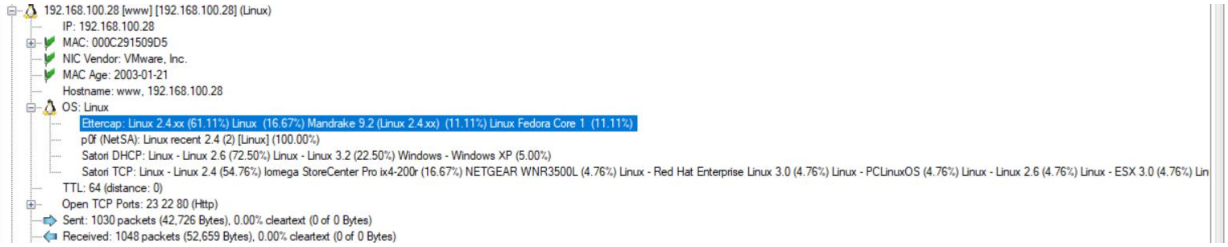
Filter keyword: 192.168.100.5
☐ Case sensitive ExactPhrase Any column

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Timestamp
150	Opening ASCII mode data connection for ...	5051	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:03 UTC
150	Opening ASCII mode data connection for ...	5145	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:19 UTC
200	PORT command successful.	5048	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:03 UTC
200	PORT command successful.	5142	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:19 UTC
215	Windows_NT	5019	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:20:54 UTC
220	Microsoft FTP Service	4945	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:20:37 UTC
221		5175	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:27 UTC
226	Transfer complete.	5062	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:03 UTC
226	Transfer complete.	5158	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:21:20 UTC
230	Anonymous user logged in.	5016	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:20:54 UTC
331	Anonymous access allowed, send identity...	4980	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	2011-10-07 18:20:49 UTC
DHCP Option 12 Hostname	xp	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC
DHCP Option 12 Hostname	www	67	192.168.100.28 [www] (Linux)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:11:35 UTC
DHCP Option 60 Vendor Code	MSFT 5.0	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC
DHCP Option 81 Domain	xp.	3	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	192.168.100.5 []	UDP 67	2011-10-07 18:10:50 UTC
DHCP Option 81 Domain		4	192.168.100.5 []	UDP 67	192.168.100.26 [xp] [xp.] (Windows)	UDP 68	2011-10-07 18:10:50 UTC
DHCP Option 81 Domain		9	192.168.100.5 []	UDP 67	255.255.255.255	UDP 68	2011-10-07 18:10:58 UTC
DHCP Option 81 Domain		5219	192.168.100.5 [] (Windows)	UDP 67	255.255.255.255	UDP 68	2011-10-07 18:22:30 UTC
LIST		5050	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:03 UTC
PASS	yeah@right.com	5014	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:54 UTC
PORT	192,168,100,27,144,208	5047	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:03 UTC
PORT	192,168,100,27,218,58	5141	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:19 UTC
QUIT		5174	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:27 UTC
RETR	Budget.txt	5144	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:19 UTC
SYST		5018	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:54 UTC
USER	anonymous	4979	192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:49 UTC

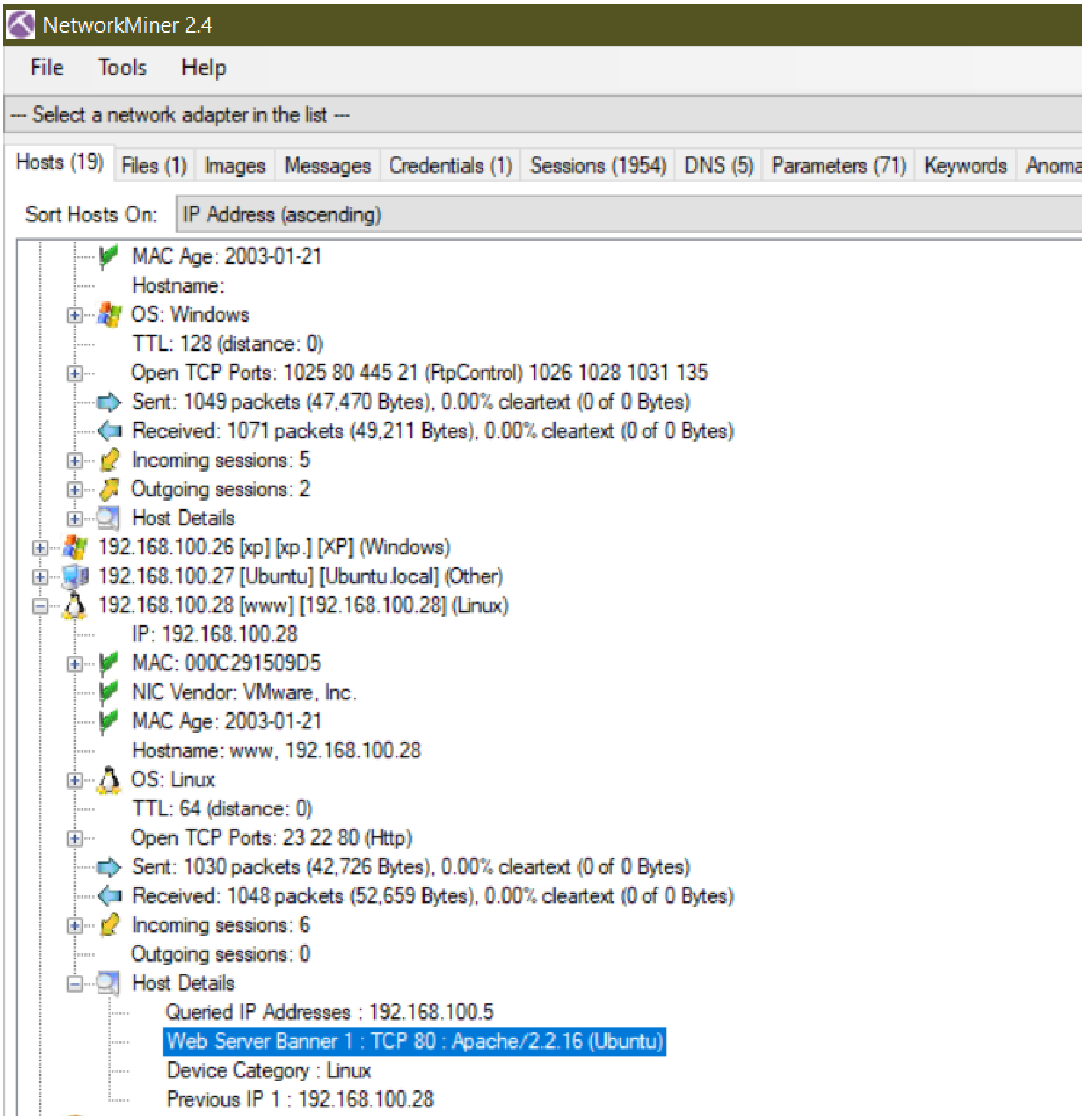
Filename	MD5
Network-...	d83a55...

3. what computer (refer by OS name and last octet of IP address) is running a web server?

192.168.100.28 (Linux 2.4.xx (61.11%) Linux (16.67%) Mandrake 9.2 (Linux 2.4.xx) (11.11%) Linux Fedora Core 1 (11.11%) 2.6.17) is the webserver because the Web Server Banner is 1 : TCP 80 : Apache/2.2.16 (Ubuntu)



```
192.168.100.28 [www] [192.168.100.28] (Linux)
    IP: 192.168.100.28
    MAC: 000C291509D5
    NIC Vendor: VMware, Inc.
    MAC Age: 2003-01-21
    Hostname: www, 192.168.100.28
    OS: Linux
        Ettercap: Linux 2.4.xx (61.11%) Linux  (16.67%) Mandrake 9.2 (Linux 2.4.xx)  (11.11%) Linux Fedora Core 1  (11.11%)
        p0f (NetSA): Linux recent 2.4 (2) [Linux] (100.00%)
        Satori DHCP: Linux - Linux 2.6 (72.50%) Linux - Linux 3.2 (22.50%) Windows - Windows XP (5.00%)
        Satori TCP: Linux - Linux 2.4 (54.76%) Iomega StoreCenter Pro ix4-200r (16.67%) NETGEAR WNR3500L (4.76%) Linux - Red Hat Enterprise Linux 3.0 (4.76%) Linux - PCLinuxOS (4.76%) Linux - Linux 2.6 (4.76%) Linux - ESX 3.0 (4.76%) Lin
    TTL: 64 (distance: 0)
    Open TCP Ports: 23 22 80 (Http)
    Sent: 1030 packets (42,726 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 1048 packets (52,659 Bytes), 0.00% cleartext (0 of 0 Bytes)
```

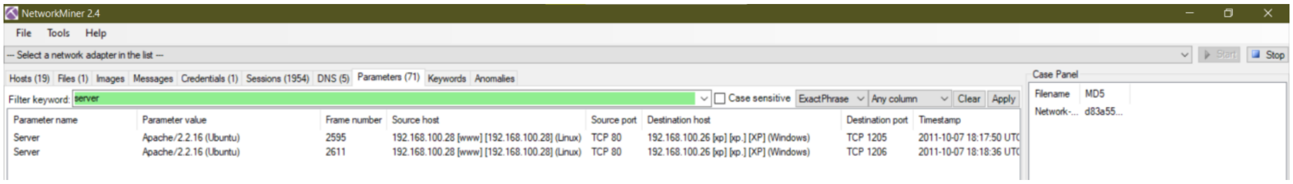


Sort Hosts On: IP Address (ascending)

```
MAC Age: 2003-01-21
Hostname:
OS: Windows
TTL: 128 (distance: 0)
Open TCP Ports: 1025 80 445 21 (FtpControl) 1026 1028 1031 135
Sent: 1049 packets (47,470 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 1071 packets (49,211 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 5
Outgoing sessions: 2
Host Details
192.168.100.26 [xp] [xp.] [XP] (Windows)
192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)
192.168.100.28 [www] [192.168.100.28] (Linux)
    IP: 192.168.100.28
    MAC: 000C291509D5
    NIC Vendor: VMware, Inc.
    MAC Age: 2003-01-21
    Hostname: www, 192.168.100.28
    OS: Linux
    TTL: 64 (distance: 0)
    Open TCP Ports: 23 22 80 (Http)
    Sent: 1030 packets (42,726 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 1048 packets (52,659 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 6
    Outgoing sessions: 0
    Host Details
        Queried IP Addresses : 192.168.100.5
        Web Server Banner 1 : TCP 80 : Apache/2.2.16 (Ubuntu)
        Device Category : Linux
        Previous IP 1 : 192.168.100.28
```

Which computer(s) accessed this webserver?

192.168.100.26 is accessing this web server.



Filter keyword: server

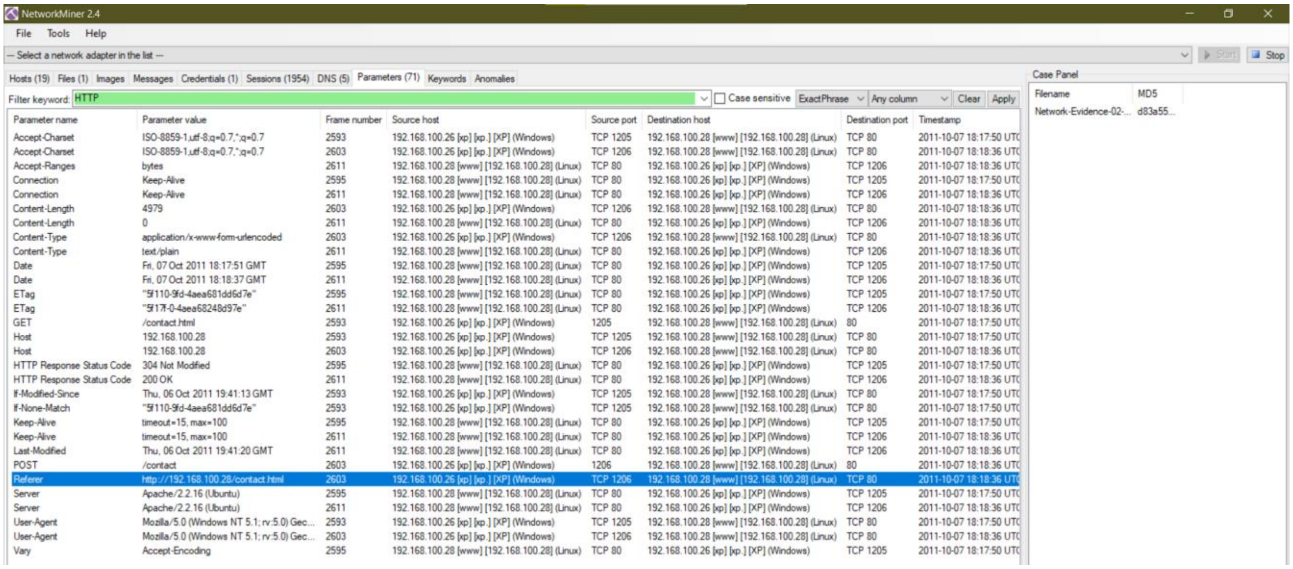
□ Case sensitive

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Timestamp
Server	Apache/2.2.16 (Ubuntu)	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
Server	Apache/2.2.16 (Ubuntu)	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC

Filename	MD5
Network-...	d83a55...

How do you know a webpage was accessed? What was the file name of the web page accessed?

By adding the “HTTP” filter keyword we can see that 192.168.100.26 is accessing a webpage “http://192.168.100.28/contact.html”



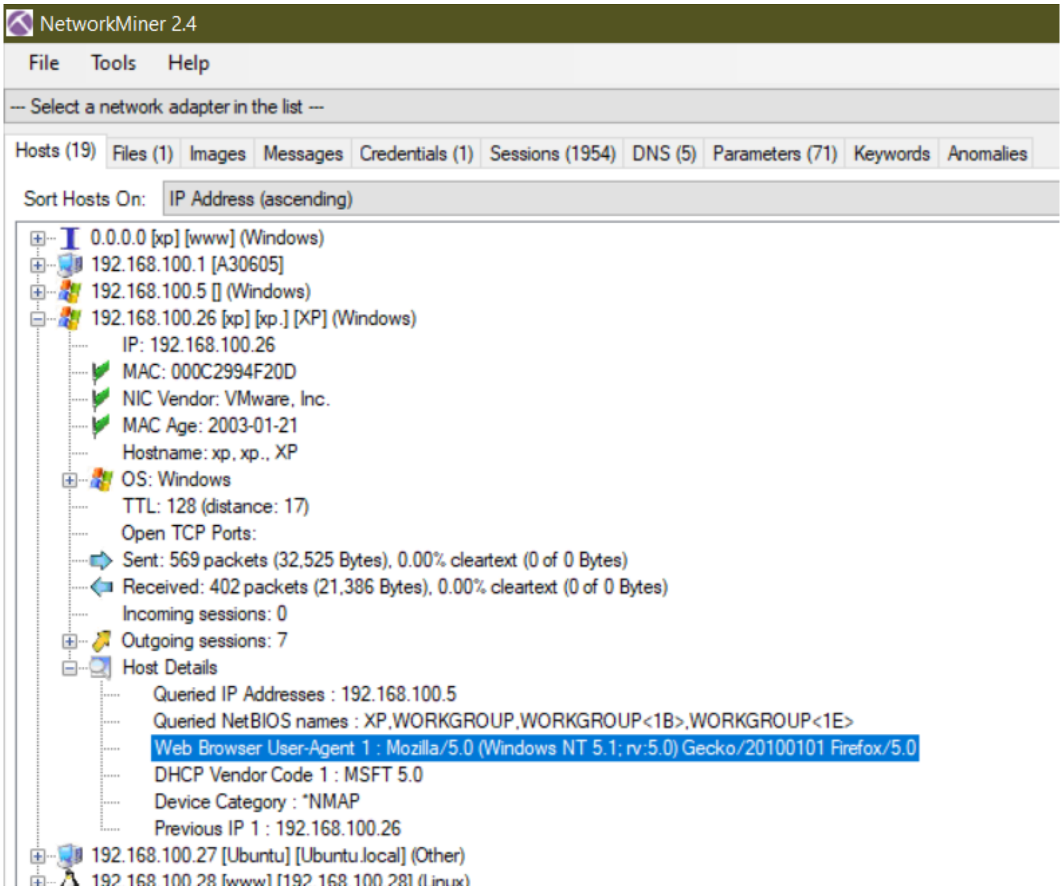
Filter keyword: HTTP ☐ Case sensitive ExactPhrase Any column

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Timestamp
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
Accept-Ranges	bytes	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
Connection	Keep-Alive	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
Connection	Keep-Alive	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
Content-Length	4979	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
Content-Length	0	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
Content-Type	application/x-www-form-urlencoded	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
Content-Type	text/plain	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
Date	Fri, 07 Oct 2011 18:17:51 GMT	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
Date	Fri, 07 Oct 2011 18:18:37 GMT	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
ETag	"5f110-9fd-4aea681dd6d7e"	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
ETag	"5f17f-0-4aea68248d97e"	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
GET	/contact.html	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	1205	192.168.100.28 [www] [192.168.100.28] (Linux)	80	2011-10-07 18:17:50 UTC
Host	192.168.100.28	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
Host	192.168.100.28	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
HTTP Response Status Code	304 Not Modified	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
HTTP Response Status Code	200 OK	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
If-Modified-Since	Thu, 06 Oct 2011 19:41:13 GMT	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
If-None-Match	"5f110-9fd-4aea681dd6d7e"	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
Keep-Alive	timeout=15, max=100	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
Keep-Alive	timeout=15, max=100	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
Last-Modified	Thu, 06 Oct 2011 19:41:20 GMT	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
POST	/contact	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	1206	192.168.100.28 [www] [192.168.100.28] (Linux)	80	2011-10-07 18:18:36 UTC
Referer	http://192.168.100.28/contact.html	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
Server	Apache/2.2.16 (Ubuntu)	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
Server	Apache/2.2.16 (Ubuntu)	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
User-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gec...	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
User-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gec...	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
Vary	Accept-Encoding	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC

Filename	MD5
Network-Evidence-02-...	d83a55...

What web browser was the user running?

192.168.100.26 is using Web Browser User-Agent 1: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0

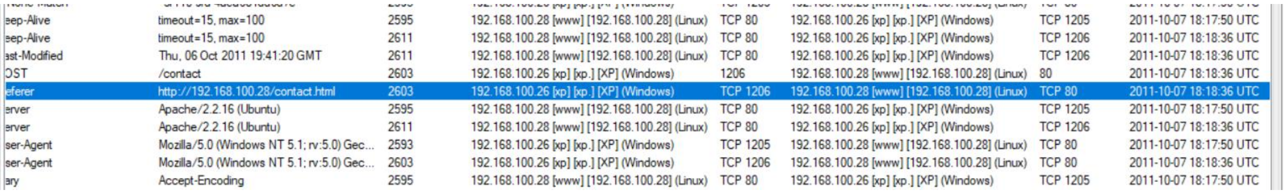


Sort Hosts On: IP Address (ascending)

```
⊞ 0.0.0.0 [xp] [www] (Windows)
⊞ 192.168.100.1 [A30605]
⊞ 192.168.100.5 [] (Windows)
⊟ 192.168.100.26 [xp] [xp.] [XP] (Windows)
      IP: 192.168.100.26
      MAC: 000C2994F20D
      NIC Vendor: VMware, Inc.
      MAC Age: 2003-01-21
      Hostname: xp, xp., XP
    ⊞ OS: Windows
      TTL: 128 (distance: 17)
      Open TCP Ports:
      Sent: 569 packets (32,525 Bytes), 0.00% cleartext (0 of 0 Bytes)
      Received: 402 packets (21,386 Bytes), 0.00% cleartext (0 of 0 Bytes)
      Incoming sessions: 0
    ⊞ Outgoing sessions: 7
    ⊟ Host Details
          Queried IP Addresses : 192.168.100.5
          Queried NetBIOS names : XP,WORKGROUP,WORKGROUP<1B>,WORKGROUP<1E>
          Web Browser User-Agent 1 : Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
          DHCP Vendor Code 1 : MSFT 5.0
          Device Category : *NMAP
          Previous IP 1 : 192.168.100.26
⊞ 192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)
⊞ 192.168.100.28 [www] [192.168.100.28] (Linux)
```

4. At what time did the access occur?

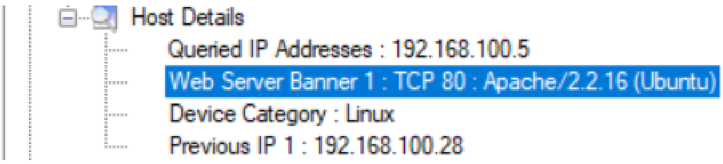
2011-10-07 18:18:36 UTC



eep-Alive	timeout=15, max=100	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
eep-Alive	timeout=15, max=100	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
ast-Modified	Thu, 06 Oct 2011 19:41:20 GMT	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
OST	/contact	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	1206	192.168.100.28 [www] [192.168.100.28] (Linux)	80	2011-10-07 18:18:36 UTC
eferer	http://192.168.100.28/contact.html	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
erver	Apache/2.2.16 (Ubuntu)	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC
erver	Apache/2.2.16 (Ubuntu)	2611	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	2011-10-07 18:18:36 UTC
ser-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gec...	2593	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:17:50 UTC
ser-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gec...	2603	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1206	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	2011-10-07 18:18:36 UTC
ary	Accept-Encoding	2595	192.168.100.28 [www] [192.168.100.28] (Linux)	TCP 80	192.168.100.26 [xp] [xp.] [XP] (Windows)	TCP 1205	2011-10-07 18:17:50 UTC

5. What webserver application was running? (include version number)

Apache/2.2.16 (Ubuntu)



```
⊟ Host Details
      Queried IP Addresses : 192.168.100.5
      Web Server Banner 1 : TCP 80 : Apache/2.2.16 (Ubuntu)
      Device Category : Linux
      Previous IP 1 : 192.168.100.28
```

6. what did the attacker do once on the FTP server?

The attacker used the following commands:

USER to send the “anonymous” send username.

PASS to send the “yeah@right.com” password.

SYST to return system type.

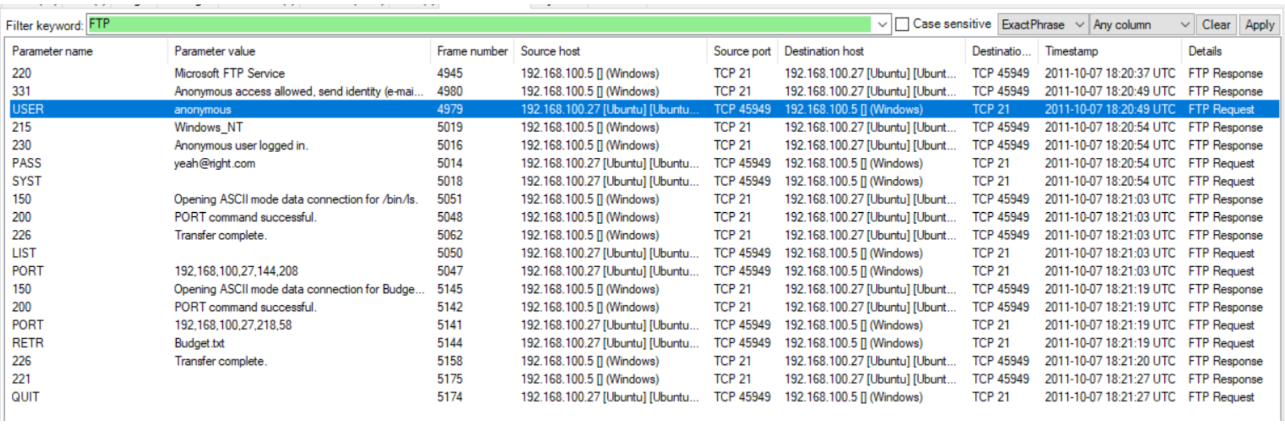
LIST to list remote files.

PORT to open a data port.

PORT to open a data port.

RETR to retrieve the “Budget.txt” remote file.

QUIT to terminate the connection.

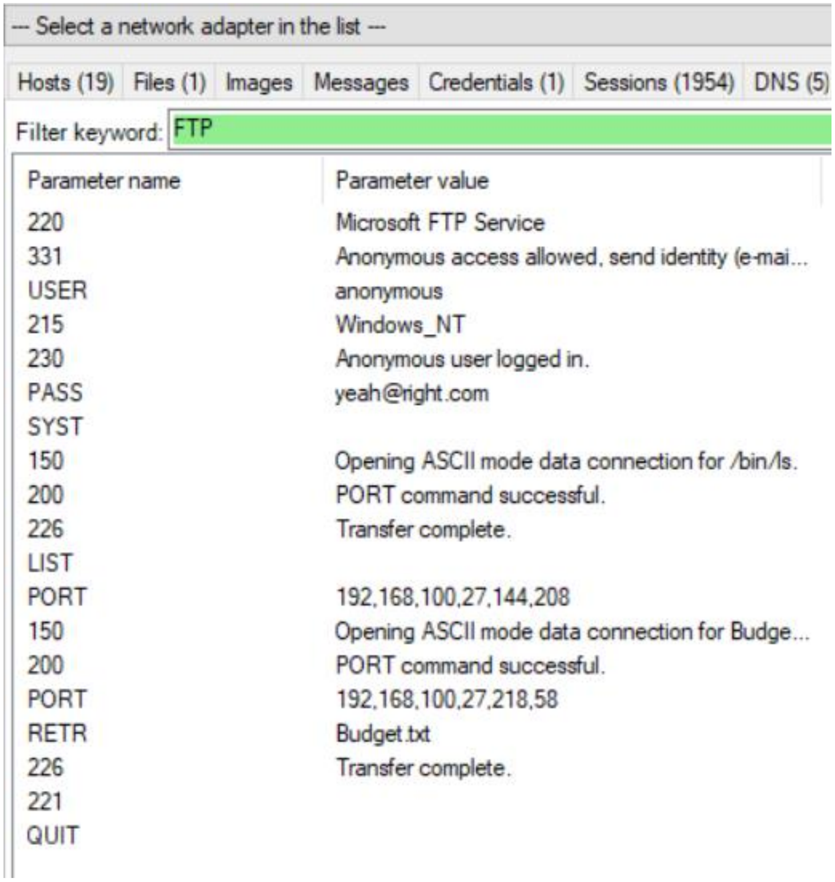


Filter keyword: FTP ☐ Case sensitive ExactPhrase Any column

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destinatio...	Timestamp	Details
220	Microsoft FTP Service	4945	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:20:37 UTC	FTP Response
331	Anonymous access allowed, send identity (e-mai...	4980	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:20:49 UTC	FTP Response
USER	anonymous	4979	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:49 UTC	FTP Request
215	Windows_NT	5019	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:20:54 UTC	FTP Response
230	Anonymous user logged in.	5016	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:20:54 UTC	FTP Response
PASS	yeah@right.com	5014	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:54 UTC	FTP Request
SYST		5018	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:20:54 UTC	FTP Request
150	Opening ASCII mode data connection for /bin/ls.	5051	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:03 UTC	FTP Response
200	PORT command successful.	5048	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:03 UTC	FTP Response
226	Transfer complete.	5062	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:03 UTC	FTP Response
LIST		5050	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:03 UTC	FTP Request
PORT	192,168,100,27,144,208	5047	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:03 UTC	FTP Request
150	Opening ASCII mode data connection for Budge...	5145	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:19 UTC	FTP Response
200	PORT command successful.	5142	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:19 UTC	FTP Response
PORT	192,168,100,27,218,58	5141	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:19 UTC	FTP Request
RETR	Budget.txt	5144	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:19 UTC	FTP Request
226	Transfer complete.	5158	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:20 UTC	FTP Response
221		5175	192.168.100.5 [] (Windows)	TCP 21	192.168.100.27 [Ubuntu] [Ubunt...	TCP 45949	2011-10-07 18:21:27 UTC	FTP Response
QUIT		5174	192.168.100.27 [Ubuntu] [Ubuntu...	TCP 45949	192.168.100.5 [] (Windows)	TCP 21	2011-10-07 18:21:27 UTC	FTP Request

7. How many commands were run on the ftp server?

8: 1.USER, 2. PASS, 3. SYST, 4. LIST, 5. PORT, 6. PORT, 7. RETR, 8. QUIT.



Filter keyword: FTP

Parameter name	Parameter value
220	Microsoft FTP Service
331	Anonymous access allowed, send identity (e-mai...
USER	anonymous
215	Windows_NT
230	Anonymous user logged in.
PASS	yeah@right.com
SYST	
150	Opening ASCII mode data connection for /bin/ls.
200	PORT command successful.
226	Transfer complete.
LIST	
PORT	192,168,100,27,144,208
150	Opening ASCII mode data connection for Budge...
200	PORT command successful.
PORT	192,168,100,27,218,58
RETR	Budget.txt
226	Transfer complete.
221	
QUIT	

8. What username and password were used to access the ftp server?

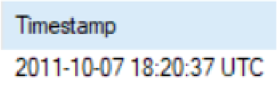
“anonymous” as username and “yeah@right.com” as the password.

9. Form what computer was the ftp server accessed?

From 192.168.100.27

10. Data and time?

2011-10-7 18:20:37 UTC



Timestamp
2011-10-07 18:20:37 UTC

11. What file was downloaded from the ftp server?

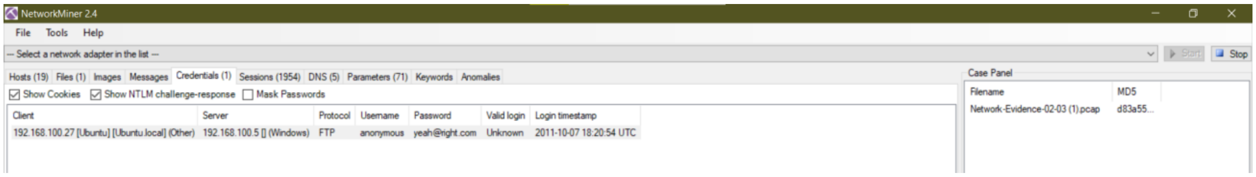
Budget.txt

12. To which computer was this file downloaded?

192.168.100.27

13. In your opinion, how technically sophisticated is the attacker? Provide evidence to support your claim.

Well, it doesn’t really matter how technically sophisticated he was, he stole the file he needed and that’s all that matters. We don’t have any personal information from him just a MAC address and a fake email address.



☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.100.27 [Ubuntu] [Ubuntu.local] (Other)	192.168.100.5 [] (Windows)	FTP	anonymous	yeah@right.com	Unknown	2011-10-07 18:20:54 UTC

Filename	MD5
Network-Evidence-02-03 (1).pcap	d83a55...