­

Digital Forensics (CS4419-CS6419)



2021SM\_CS\_6419\_FRE1A

Assignment-02

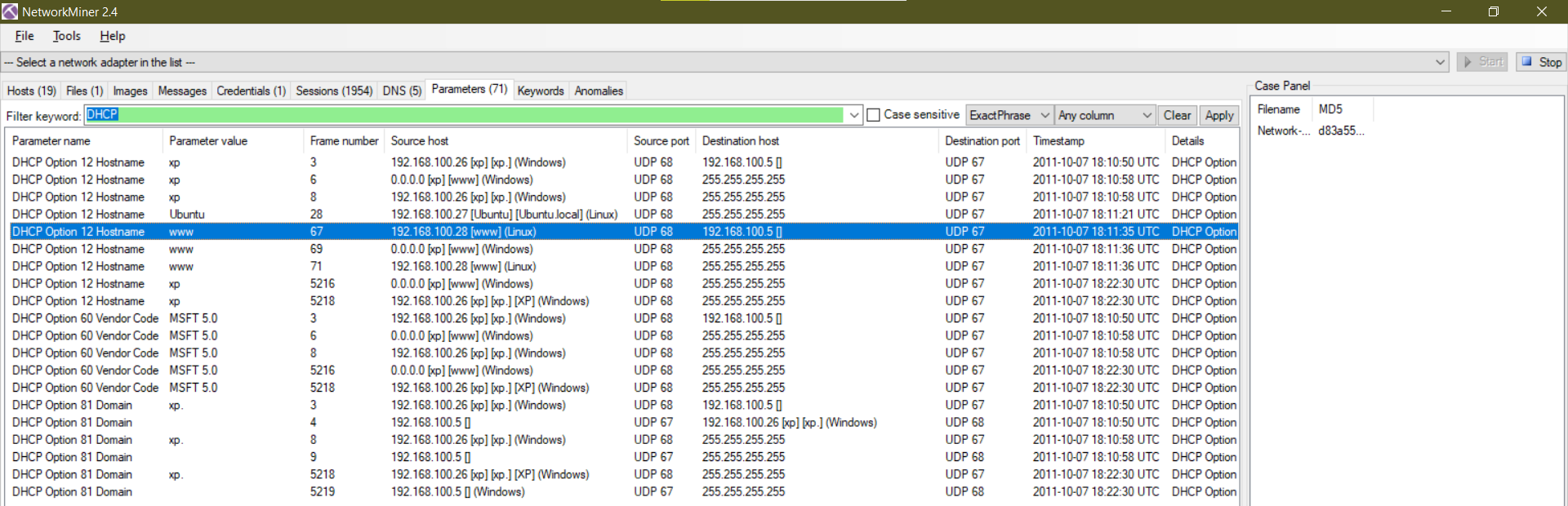
Prepared by:  
Mohammadali Rahnama

Student number:

3709515

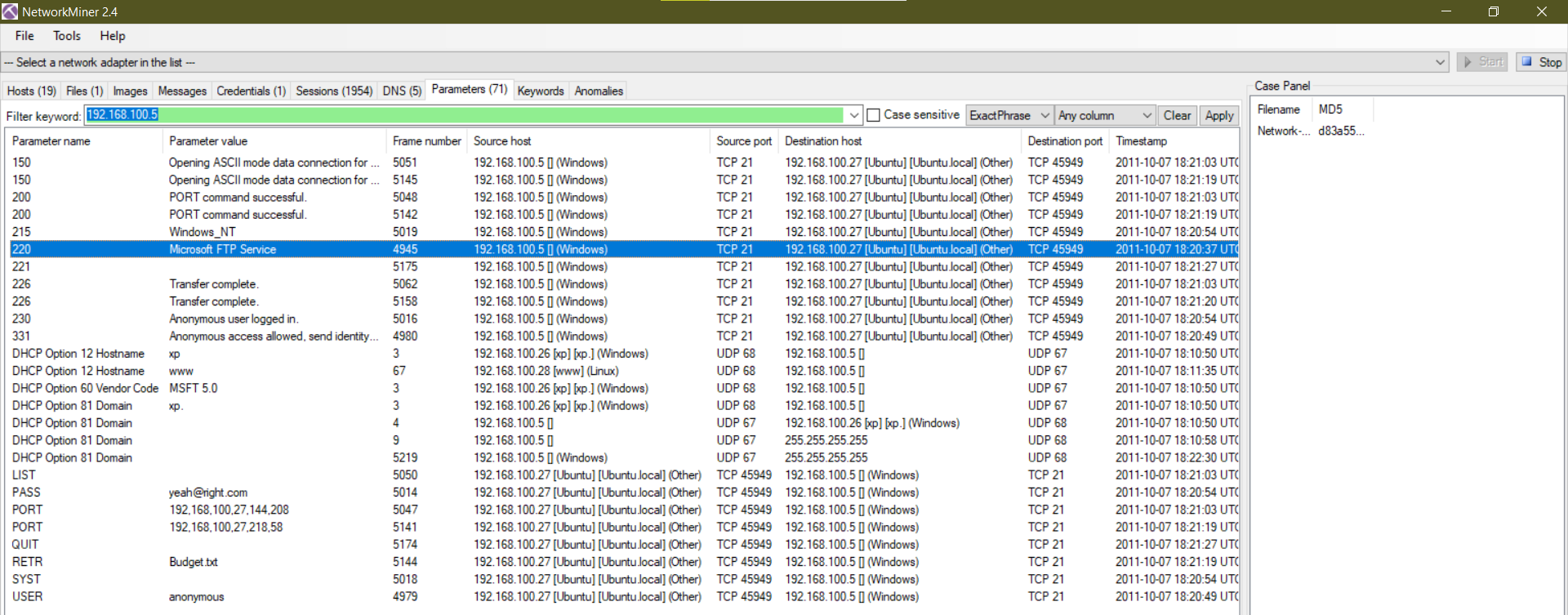
1. **What computer is serving as DHCP server? How do you know?**

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



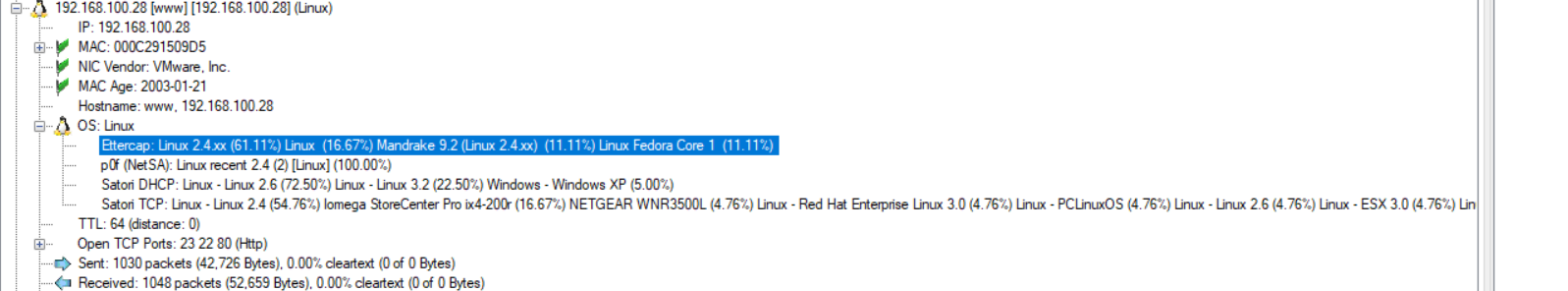
1. **What other services is the DHCP server running? How do you know?**

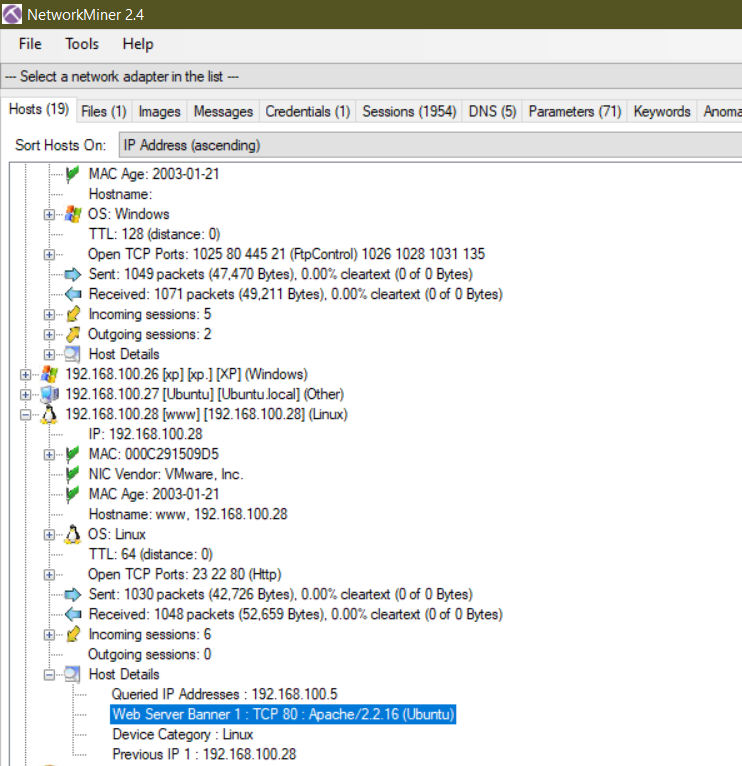
By adding the “192.168.100.5” filter keyword we can see that 192.168.100.5 is also running Microsoft FTP Service as well.



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

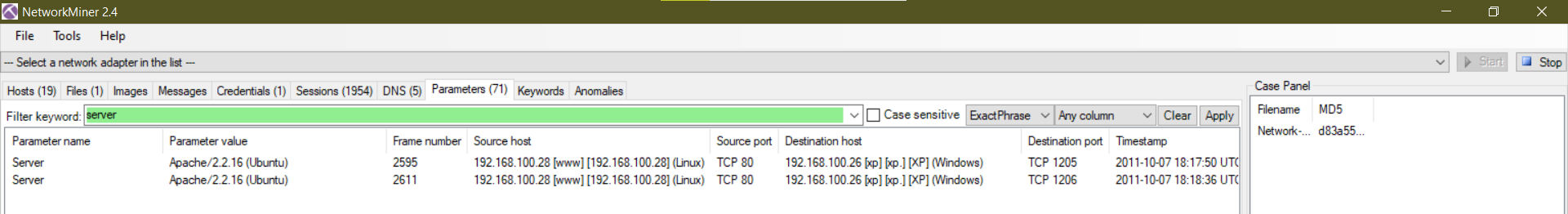
192.168.100.28 (Linux 2.4.xx (61.11%) Linux (16.67%) Mandrake 9.2 (Linux 2.4.xx) (11.11%) Linux Fedora Core 1 (11.11%) 2.6.17) is the webserver because the Web Server Banner is 1 : TCP 80 : Apache/2.2.16 (Ubuntu)





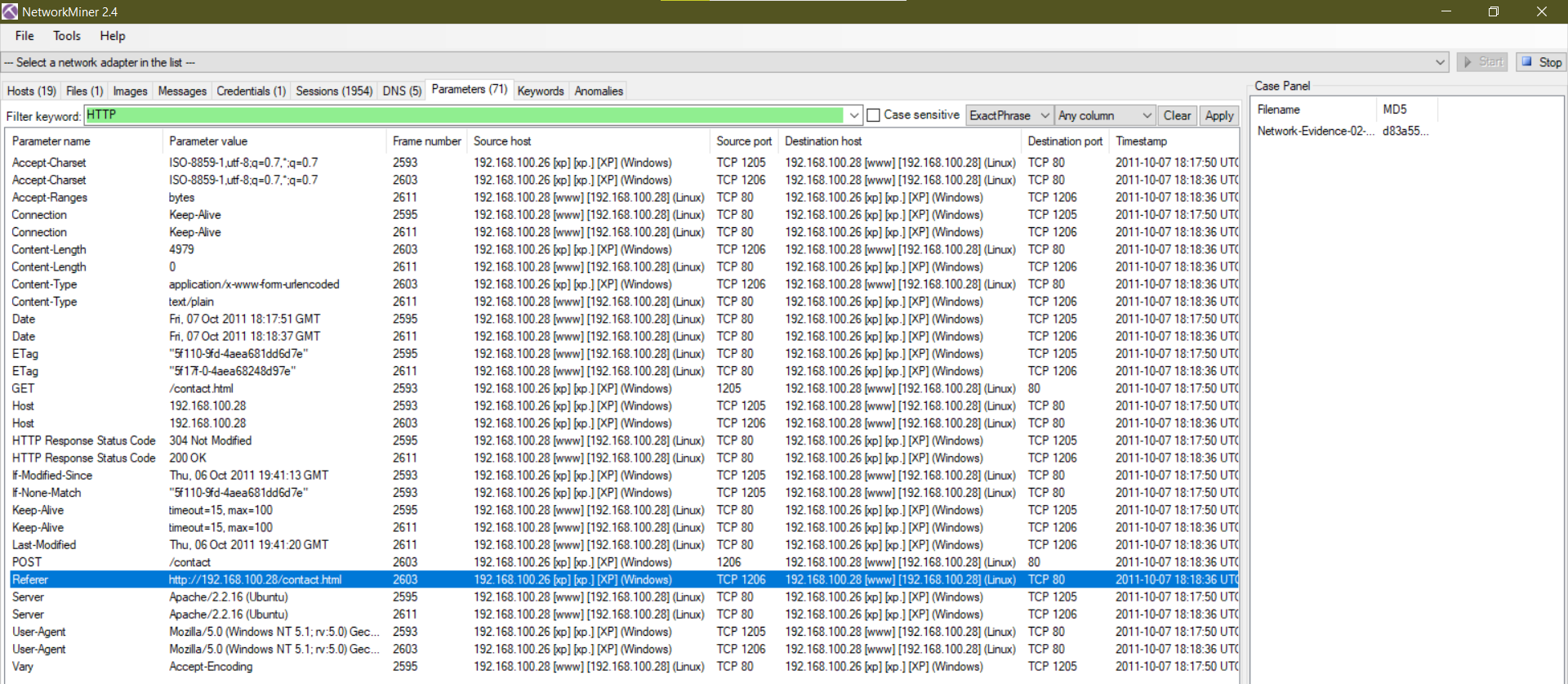
**Which computer(s) accessed this webserver?**

192.168.100.26 is accessing this web server.



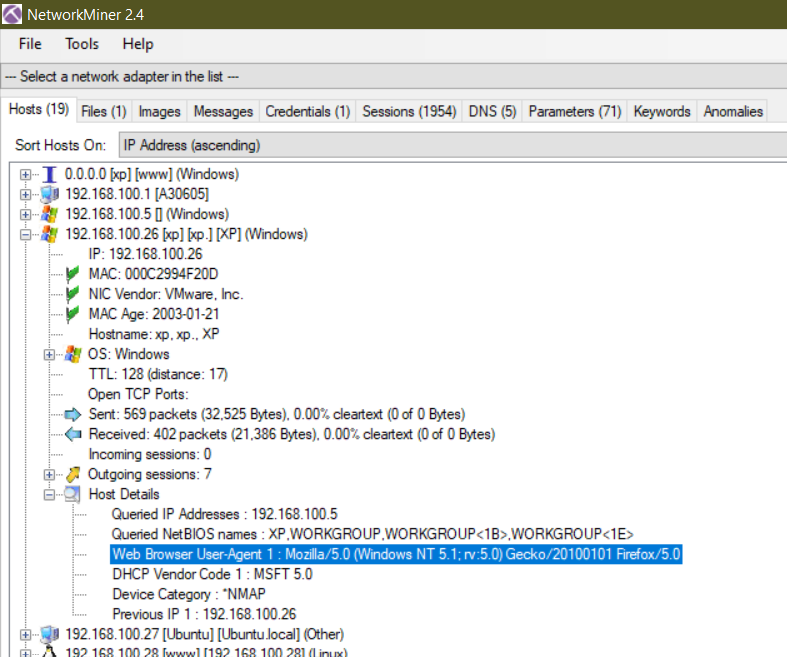
**How do you know a webpage was accessed? What was the file name of the web page accessed?**

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”



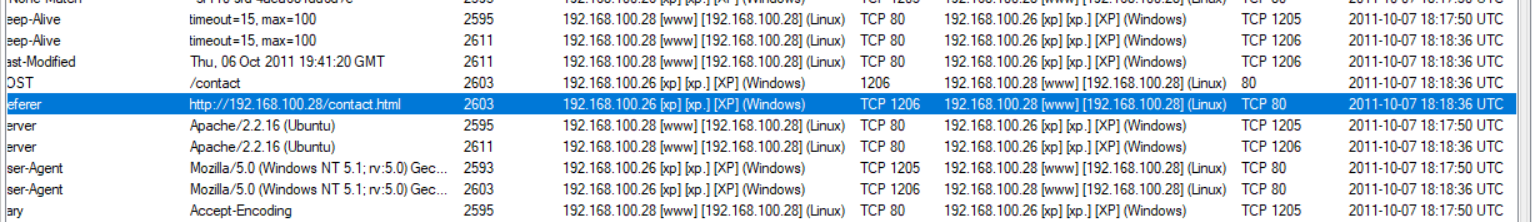
**What web browser was the user running?**

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



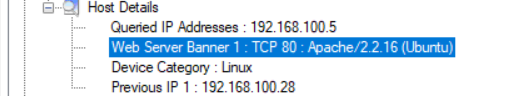
1. **At what time did the access occur?**

2011-10-07 18:18:36 UTC



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

Apache/2.2.16 (Ubuntu)



1. **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](mailto:yeah@right.com)” password.

SYST to return system type.

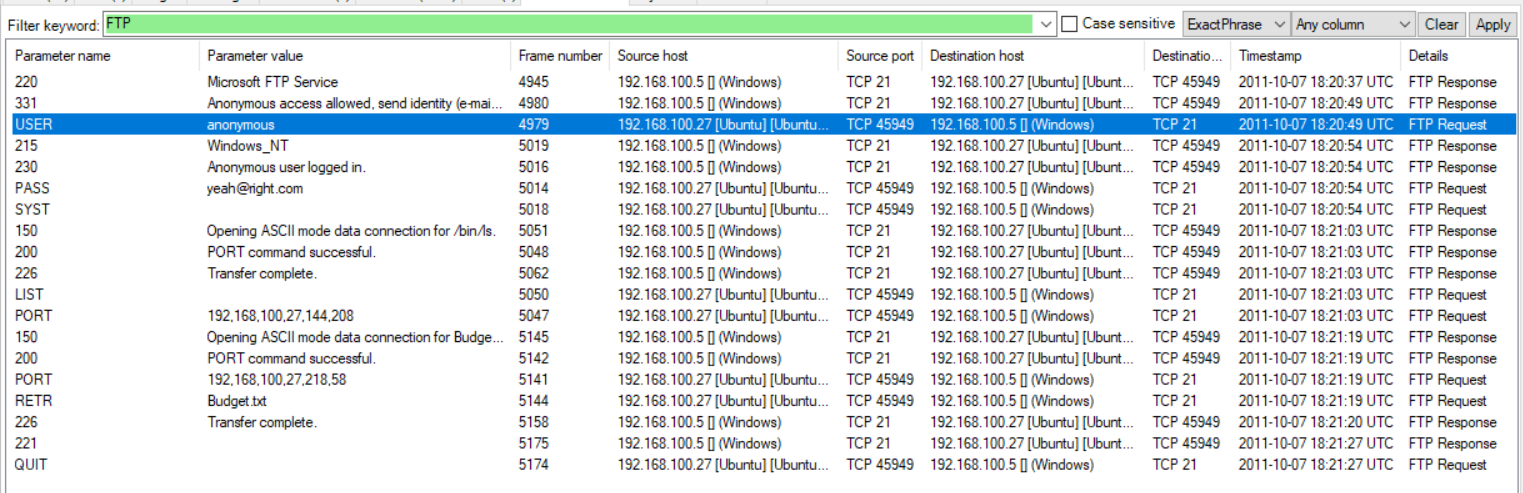
LIST to list remote files.

PORT to open a data port.

PORT to open a data port.

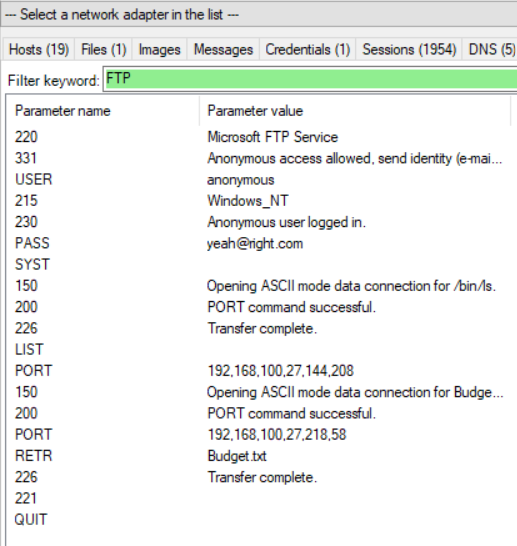
RETR to retrieve the “Budget.txt” remote file.

QUIT to terminate the connection.



1. **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.



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

“anonymous” as username and “[yeah@right.com](mailto:yeah@right.com)” as the password.

1. **Form what computer was the ftp server accessed?**

From 192.168.100.27

1. **Data and time?**

2011-10-7 18:20:37 UTC



1. **What file was downloaded from the ftp server?**

Budget.txt

1. **To which computer was this file downloaded?**

192.168.100.27

1. **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.

