

Lab 6

Authors: Daniel Gisolfi, James Ekstract

Section 1

A screen capture showing the whois information for Global Enterprises

WHOIS information for globalenterprises.com:

[Querying whois.verisign-grs.com]
[Redirected to whois.enom.com]
[Querying whois.enom.com]
[whois.enom.com]

Domain Name: GLOBALENTERPRISES.COM
Registry Domain ID: 85461309_DOMAIN_COM-VRSN
Creation Date: 2002-04-10 18:06:00Z
Registrar Registration Expiration Date: 2014-04-10 18:06:00Z
Registrar: ENOM, INC.
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252744500
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: WHOIS AGENT
Registrant Organization: HTTP://WWW.GOBALHOLDINGS.COM/GLOBALENTERPRISES.COM?UTM_SOURCE=WHOIS
Registrant Street: PO BOX 639
Registrant City: DOVER
Registrant State/Province: DE
Registrant Postal Code: 19904
Registrant Country: US
Registrant Phone: +1.800.CAR.PETS
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:

A screen capture showing LouAnne's GetConnected profile

WANT TO GET CONNECTED?



LouAnne Garfinkle

Director Global IT

Georgia Home Goods

Current: Global Enterprises

Previous: Rugs-R-Us, City of Calhoun

Education: North Georgia College

Connect

Send LouAnne InMail

500+
connections

Background



Summary

Top Information Technology Professional. At Global Enterprises since 2009. Recipient of 2010 Top Contributors Award. Frequent speaker at conferences and user groups. Writes a blog: IT Insights. Currently pursuing MBA. Married with 2 high school age daughters.

A screen capture showing the first blog entry



I am a 21 year veteran of Information Technology. I started my career when IT was called DP: Data Processing and saw the last of the IBM 029 card punch and the first of the Cathode Ray Tube (CRT). This blog represents my personal musing and observations and not those of my employer or any other company or individual. You are welcome and invited to comment on my post and to share your own thoughts, insights, and observations.

FRIDAY,
AUGUST 16, 2013

FIREWALL FRIDAY



How tough could it be? After all a firewall is pretty much a two port router with some extra code. But, we waited for a Friday anyway so we would have a couple of light days in case of problems. And, of course, we had a back-up plan. In an effort to save money we had chosen pfSense 2.0, a stable, steady and steady open source firewall with a large following, good reputation and we tested the firewall configuration in the lab prior to actual installation. I am still unclear why we decided to install the pfSense software on a clean machine even though we had it running great in the lab, but we did. During the live installation, it stuck at "Trying to mount root from ufs:/dev/ufs/pfsense0". This was not a problem we had during the installation in the lab nor had we ever

A screen capture showing the second blog entry



FRIDAY,
NOVEMBER 29, 2013

I am a 21 year veteran of Information Technology. I started my career when IT was called DP: Data Processing and saw the last of the IBM 029 card punch and the first of the Cathode Ray Tube (CRT). This blog represents my personal musing and observations and not those of my employer or any other company or individual. You are welcome and invited to comment on my post and to share your own thoughts, insights, and observations.

OPEN SOURCE... DOES IT MAKE SENSE?



Of course it makes "cents", but does it make "sense"? My CFO has asked me a number of times "What don't you understand about free?" But it is still a question that I think needs asking. I have been around IT for over two decades, but a lot of our new hires don't even know about products and services that you pay for with 800 numbers to call when there is a problem and well-trained support engineers that will actually *come to your place of business if there is a problem!* How weird is that? In the last 12 months we have moved from a real solid name-brand firewall to pfSense, we have migrated to a Bring Your Own Device policy that saves the company money on the devices, but is a support and security nightmare, we have an open source mail

Firewall Software

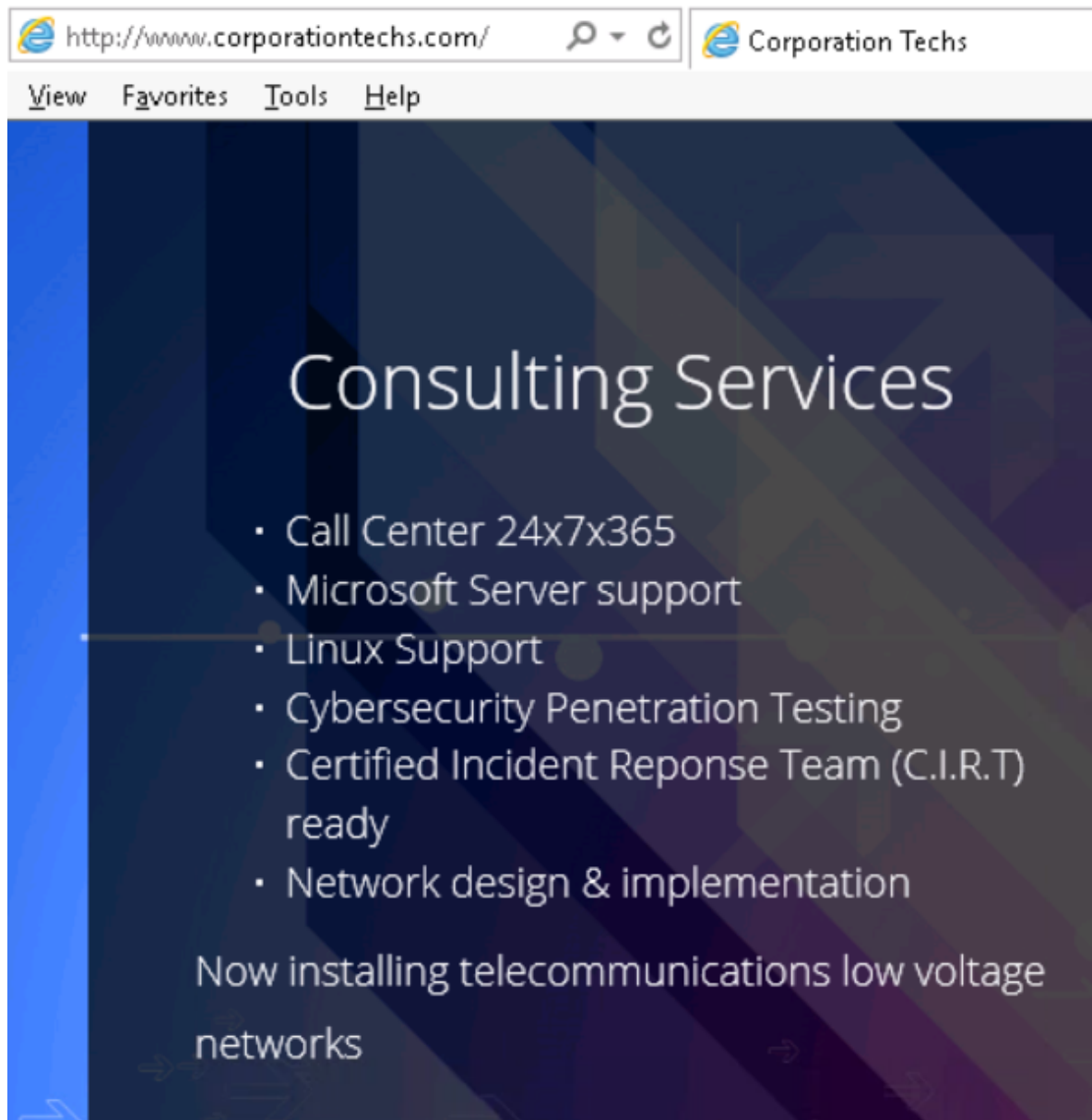
Version: 2.4.4

site: <https://www.pfsense.org/download/>

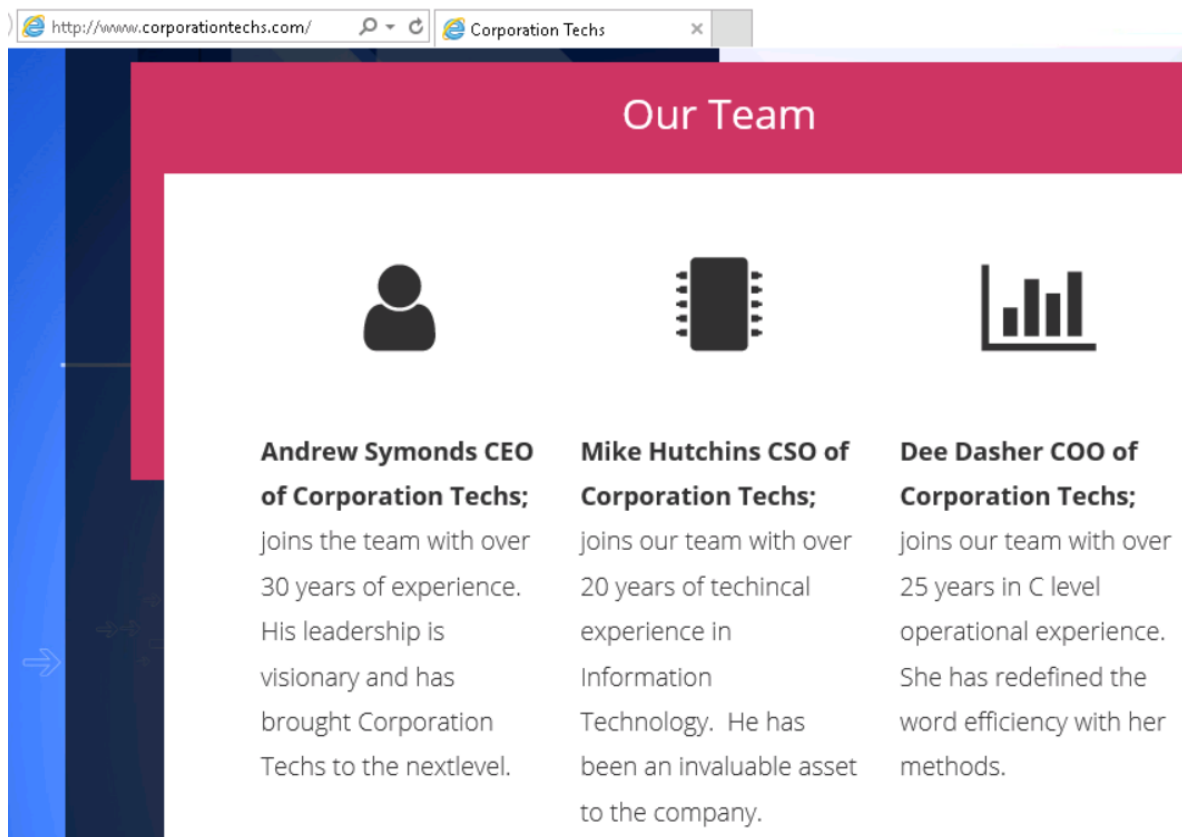
Section 2

Part 1

The services offered by the company "Corporation Techs"



The corporate officers of Corporation Techs



Details about each corporate officer of Corporation Techs from LinkedIn

Name	Position	Alma Mater	Years Attended	Location	Longest Company Career
Andrew Symonds	CEO	San Diego State University		Addison, TX	Wodash Incorporated
Mike Hutchins	CSO	Virginia Tech	1992-1996	Addison, TX	Aegis Secured
Dee Dasher	COO	Texas State University	1985-1989	Addison, TX	Dante's Inc

The search results for Andrew Symonds' LinkedIn profile using Google's advanced search operators

https://www.google.com/search?sour Corporation Techs allintext:Andrew Symonds ...

dating our Terms of Service. Get to know our new Terms before they take effect on March 31, 2020. Review Got it

Google

allintext:Andrew Symonds Corporation Techs site:www.linkedin.com

All News Maps Images Videos More Settings Tools

About 34 results (0.34 seconds)

www.linkedin.com › andrew-symonds-72019b146
Andrew Symonds - CEO - Corporation Techs | LinkedIn
View Andrew Symonds' profile on LinkedIn, the world's largest professional community. Andrew has 5 jobs listed on their profile. See the complete profile on ...

www.linkedin.com › andrew-symonds-35997715a
Andrew Symonds - Support Specialist - Transresources PVT ...
Fresno, California - Transresources PVT LTD
Andrew Symonds. Support Specialist ... **Andrew Symonds.** CEO at **Corporation Techs** ... 96 others named **Andrew Symonds** are on LinkedIn. See others named ...

www.linkedin.com › andrew-symonds-80544a139
Andrew Symonds - Technology Consultant - confidential ...
Piscataway, New Jersey - confidential
Andrew Symonds. IT Specialist. confidential. Piscataway, New ... #India #Hanuman. Liked by **Andrew Symonds** **Andrew Symonds.** CEO at **Corporation Techs.**
IPNetInfo

The individualized Google search using advanced operators

allintitle:Dee Dasher Corporation Techs site:www.linkedin.com

All News Maps Images Shopping More Settings Tools

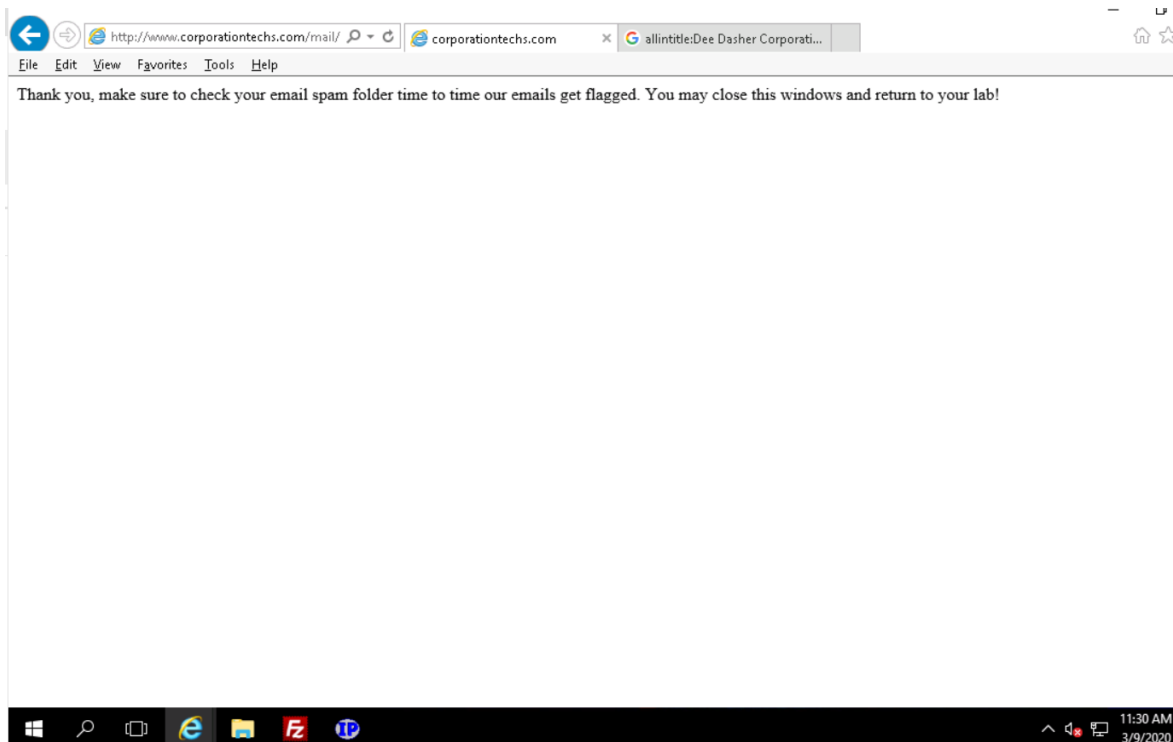
About 1 results (0.30 seconds)

www.linkedin.com › dee-dasher-4901a0146
Dee Dasher - COO - Corporation Techs | LinkedIn
View Dee Dasher's profile on LinkedIn, the world's largest professional community. Dee has 5 jobs listed on their profile. See the complete profile on LinkedIn ...

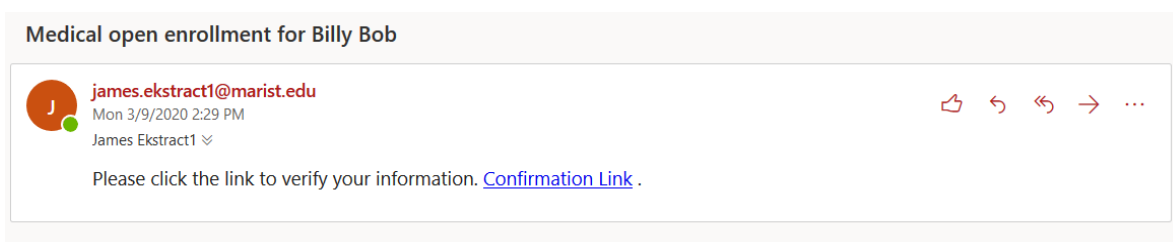
Images

Part 2

The confirmation message that appears after the contact form is submitted



The content of the contact form email



The webpage displayed after clicking the confirmation link in the above email



Part 3

The results of the nmap scan of the Corporation Techs website

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap -sV -Pn -script=http-enum www.corporationtechs.com

Starting Nmap 7.40 ( https://nmap.org ) at 2020-03-09 11:36 Pacific Daylight Time
Nmap scan report for www.corporationtechs.com (50.209.180.134)
Host is up (0.091s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-enum:
|   /mail/: Mail folder
|   /css/: Potentially interesting folder
|   /errors/: Potentially interesting directory w/ listing on 'apache/2.2.22 (debian)'
|   /images/: Potentially interesting folder
|_  /js/: Potentially interesting directory w/ listing on 'apache/2.2.22 (debian)'
|_ http-server-header: Apache/2.2.22 (Debian)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.22 seconds

C:\Users\Administrator>_

```

The WHOIS data for the suspicious IP address

IPNetInfo

File Edit View Options Help

Order	IP Address	Status	Country	Network Name	Owner Name	F
1	118.244.237.33	Succeed	China	DXTNET	Beijing Teletro...	1

```

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '118.244.0.0 - 118.244.255.255'

% Abuse contact for '118.244.0.0 - 118.244.255.255' is 'ipas@cnnic.cn'

inetnum:        118.244.0.0 - 118.244.255.255
netname:        DXTNET
descr:          Beijing Teletron Telecom Engineering Co., Ltd.
descr:          Jian Guo Road, Chaoyang District, Beijing, PR.China
admin-c:        BW904-AP
tech-c:         BW904-AP
country:        CN
mnt-by:         MAINT-CNNIC-AP
mnt-lower:      MAINT-CNNIC-AP
mnt-irt:        IRT-CNNIC-CN
mnt-routes:     MAINT-CNNIC-AP
status:         ALLOCATED PORTABLE
last-modified:  2019-05-05T02:36:52Z
source:         APNIC

irt:            IRT-CNNIC-CN
address:        Beijing, China
e-mail:         ipas@cnnic.cn
abuse-mailbox:  ipas@cnnic.cn
admin-c:        IP50-AP
tech-c:         IP50-AP
auth:          # Filtered
remarks:        Please note that CNNIC is not an ISP and is not
remarks:        empowered to investigate complaints of network abuse

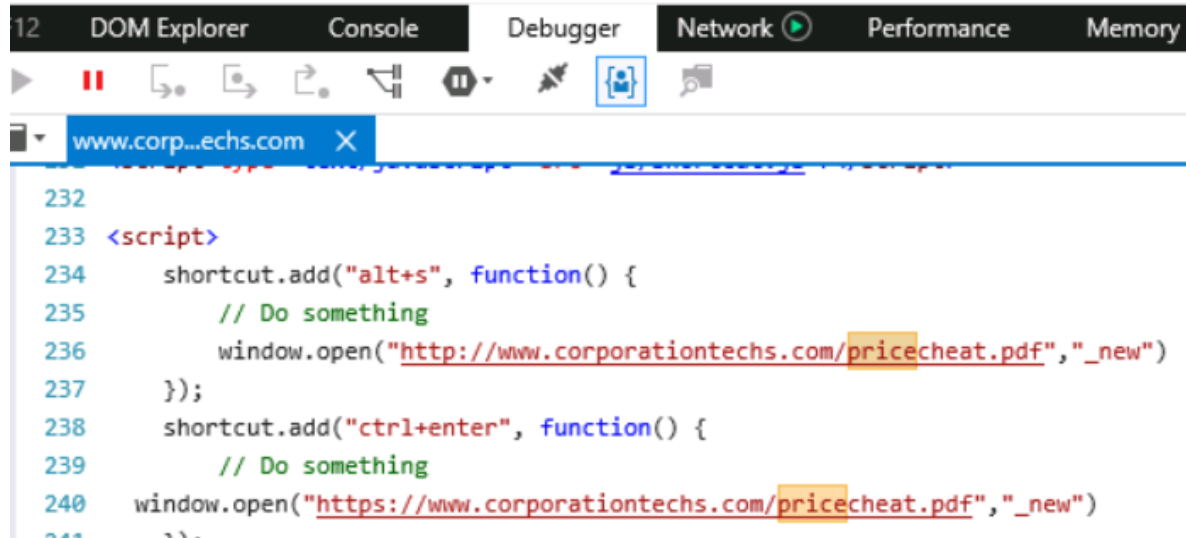
item(s), 1 Selected

```


The search results for the pricesheet in the Apache server logs, displayed in Excel

92 73.223.84.87 - [20/Aug/2017:21:11:37 -0700] "GET /pricecheat.pdf HTTP/1.1" 200 33034 "http://www.corporationtechs.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6)"

The script that will open the "pricecheat.pdf" file in the website's source code"



```
12  DOM Explorer  Console  Debugger  Network  Performance  Memory
232
233 <script>
234     shortcut.add("alt+s", function() {
235         // Do something
236         window.open("http://www.corporationtechs.com/pricecheat.pdf", "_new")
237     });
238     shortcut.add("ctrl+enter", function() {
239         // Do something
240         window.open("https://www.corporationtechs.com/pricecheat.pdf", "_new")
241     });
```

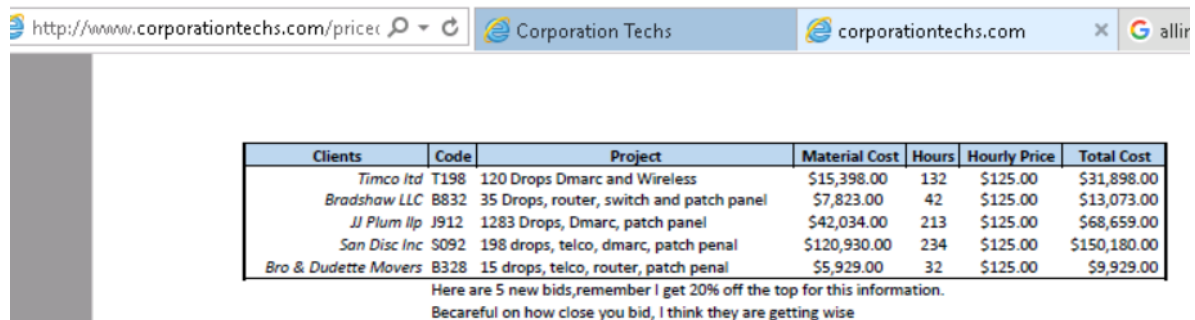
Actions necessary to open the "pricecheat.pdf" file on the Corporation Techs website"

alt + s

OR

ctrl + enter

The "pricecheat.pdf" file displayed on the Corporation Techs website after executing the necessary actions to display the file



Clients	Code	Project	Material Cost	Hours	Hourly Price	Total Cost
Timco Ltd	T198	120 Drops Dmarc and Wireless	\$15,398.00	132	\$125.00	\$31,898.00
Bradshaw LLC	B832	35 Drops, router, switch and patch panel	\$7,823.00	42	\$125.00	\$13,073.00
JJ Plum llp	J912	1283 Drops, Dmarc, patch panel	\$42,034.00	213	\$125.00	\$68,659.00
San Disc Inc	S092	198 drops, telco, dmarc, patch penal	\$120,930.00	234	\$125.00	\$150,180.00
Bro & Dudette Movers	B328	15 drops, telco, router, patch penal	\$5,929.00	32	\$125.00	\$9,929.00

Here are 5 new bids,remember I get 20% off the top for this information.
Be careful on how close you bid, I think they are getting wise