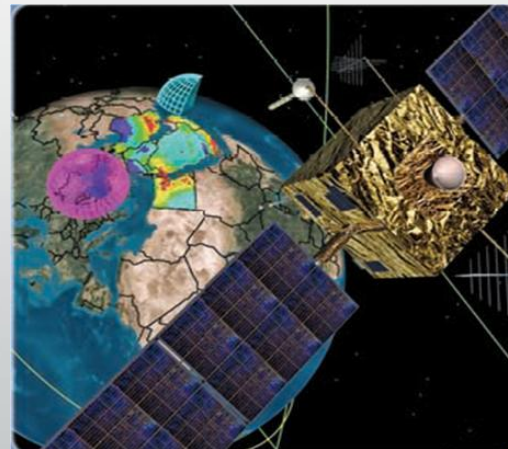


A Passive Intrusion into Analytical Graphics Inc.

Devin Trejo

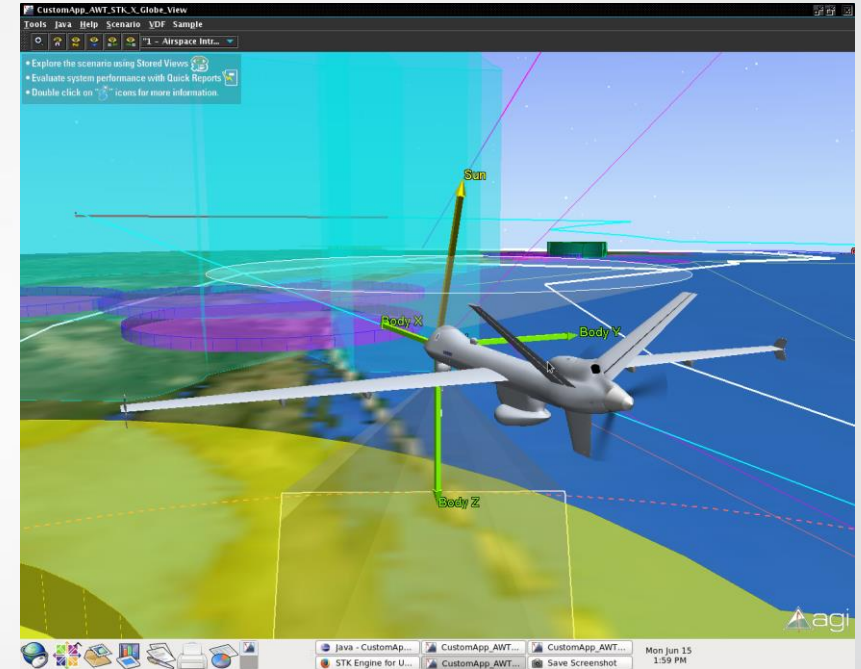
devin.trejo@temple.edu

20160208



Overview

- Background Company Information
- Passive Information Gathering Methods
- Passive Information Gathering Results
- A Quick Active? Information Gathering Result
- Concluding Summary





Background Company Information

What can we find with a typical Google Search?

Background Company Information

Wikipedia

"Analytical Graphics, Inc. (AGI) develops commercial modeling and analysis software for the aerospace, defense and intelligence communities. AGI software is used by more than 50,000 engineers, operators and analysts worldwide.

Founded in 1989, AGI's nearly 200 employees are spread between the international headquarters in Exton, Pennsylvania, with satellite offices in Washington, D.C., Colorado Springs, CO, Long Beach, CA, the UK and Singapore.[1] The current CEO is Paul Graziani.[2]" -- (Wikipedia)





Passive Information Gathering Methods

Tools Used In This Analysis.

Passive Information Gathering Methods

The Harvester

- “The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.” -- (tools.kali.org/)



Whois

- “Whois is a query and response [protocol](#) that is widely used for querying [databases](#) that store the registered users or assignees of an [Internet](#) resource, such as a [domain name](#), an [IP address](#) block, or an [autonomous system](#), but is also used for a wider range of other information.” -- ([Wikipedia](#))



Passive Information Gathering Methods

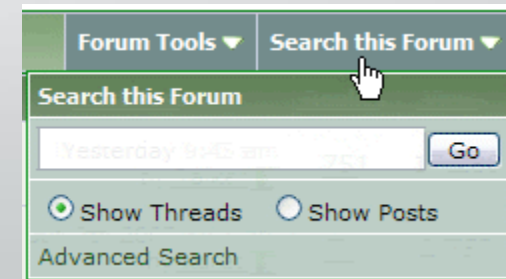
SSL Certificates

- We look to see if they have a site still running insecure connections to see if we can implement a man in the middle attack.



Forum Searching

- Look for forums where system administrators talk about their systems. Also find other resources the internal group may unitize.





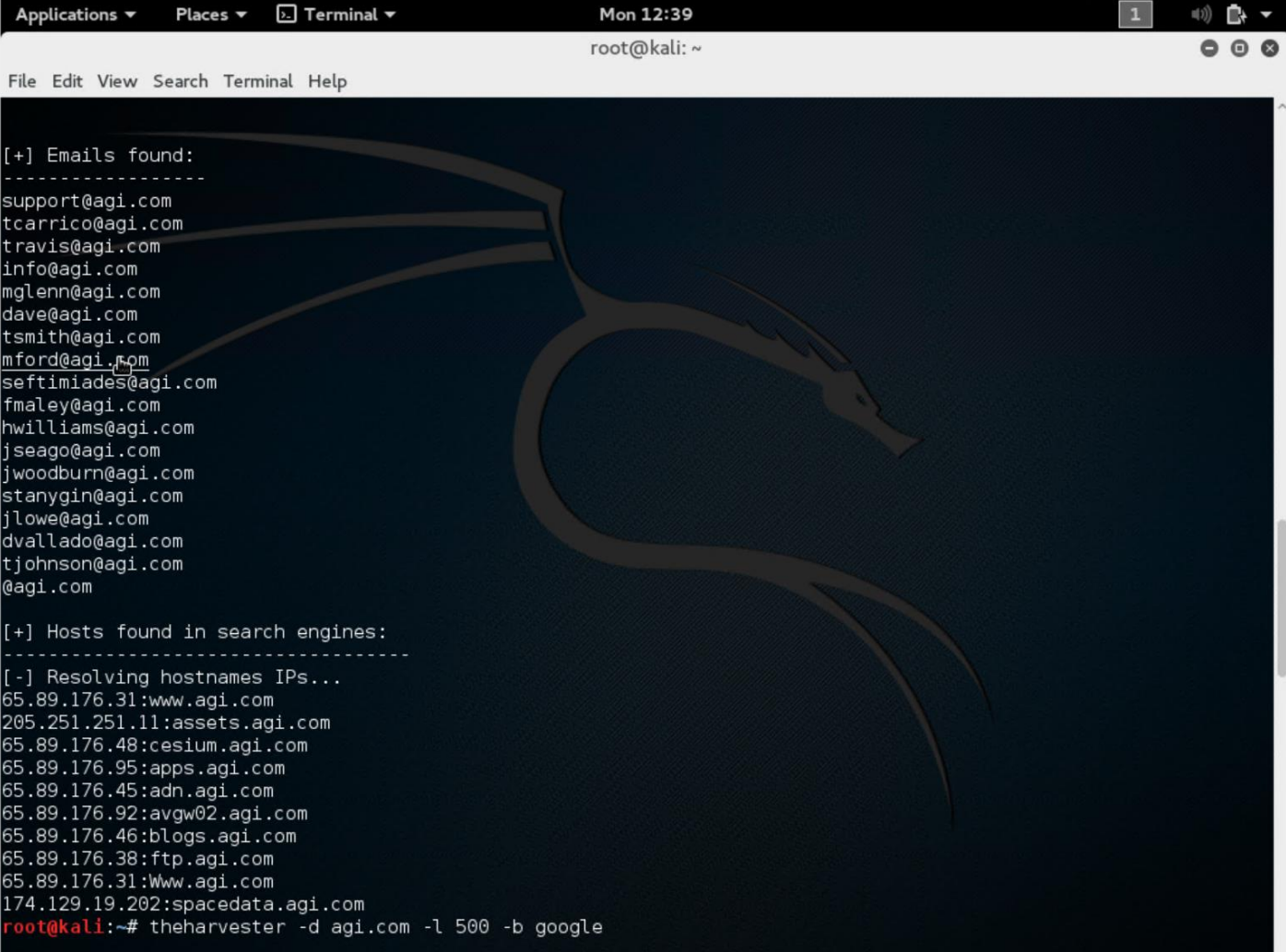
Passive Information Gathering Results

What we found in our Passive Information Gathering.

Passive Penetration Results The Harvester

Summary:

- 18 Emails
- 10 Sub-Domains:
 - Internal IP Address Space: 65.89.176.XXX
 - Other Addresses: 205.251.251.11, 174.129.19.202



```
Applications ▾ Places ▾ Terminal ▾ Mon 12:39 1
root@kali: ~

File Edit View Search Terminal Help

[+] Emails found:
-----
support@agi.com
tcarrico@agi.com
travis@agi.com
info@agi.com
mglenn@agi.com
dave@agi.com
tsmith@agi.com
mford@agi.com
seftimiades@agi.com
fmaley@agi.com
hwilliams@agi.com
jseago@agi.com
jwoodburn@agi.com
stanygin@agi.com
jlowe@agi.com
dvallado@agi.com
tjohnson@agi.com
@agi.com

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
65.89.176.31:www.agi.com
205.251.251.11:assets.agi.com
65.89.176.48:cesium.agi.com
65.89.176.95:apps.agi.com
65.89.176.45:adn.agi.com
65.89.176.92:avgw02.agi.com
65.89.176.46:blogs.agi.com
65.89.176.38:ftp.agi.com
65.89.176.31:Www.agi.com
174.129.19.202:spacedata.agi.com
root@kali:~# theharvester -d agi.com -l 500 -b google
```

Passive Penetration Results

Whois: agi.com

Summary:

- David Downs is a probably a head administrator
- Server has been around since 1994

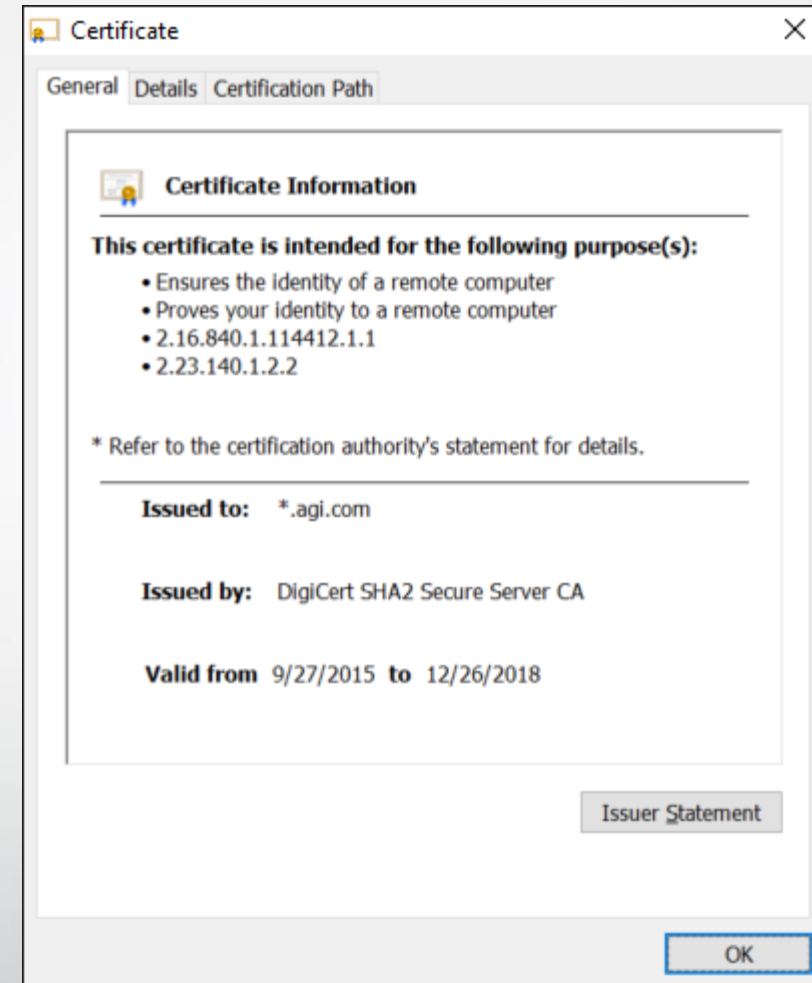
- Admin Details
 - Name: Downs, David
 - Street: 220 Valley Creek Blvd
 - City: Exton
 - State/Province: PA
 - Postal Code: 19341
 - Country: US
 - Phone: +1.6109818000
 - Email: dnsadmin@agi.com
- Tech Details:
 - <same as admin>
- Important Dates
 - Updated Date: 2015-09-02
 - Created Date: 1994-09-07
 - Registration Expiration Date: 2016-09-06
- Nameservers
 - ns3.broadwing.net - 216.140.16.252
 - ns4.broadwing.net - 216.140.17.252
- Registrar:
 - NETWORK SOLUTIONS, LLC. - <http://www.networksolutions.com/>

Passive Penetration Results

SSL Certificate agi.com

Summary:

- Using a wildcard certificate for all sub-domains. Expect secure communications between client and server.



Passive Penetration Results

Whois: 205.251.251.11

Summary:

- They use Amazon Cloud EC2 instance for holding software assets

BG:

- Amazon EC2 instances are grouped into 5 families: "General Purpose, Compute Optimized, Memory Optimized, GPU, and Storage Optimized instances" -- ([Amazon](#))

- NetRange: 205.251.192.0 - 205.251.255.255
- CIDR: 205.251.192.0/18
- NetName: AMAZON-o5
- NetHandle: NET-205-251-192-0-1
- Parent: NET205 (NET-205-0-0-0-0)
- NetType: Direct Allocation
- OriginAS: AS16509, AS39111, AS7224
- Organization: Amazon.com, Inc. (AMAZON-4)
- RegDate: 2010-08-27
- Updated: 2015-09-24

Passive Penetration Results

Whois: 174.129.19.202

Summary:

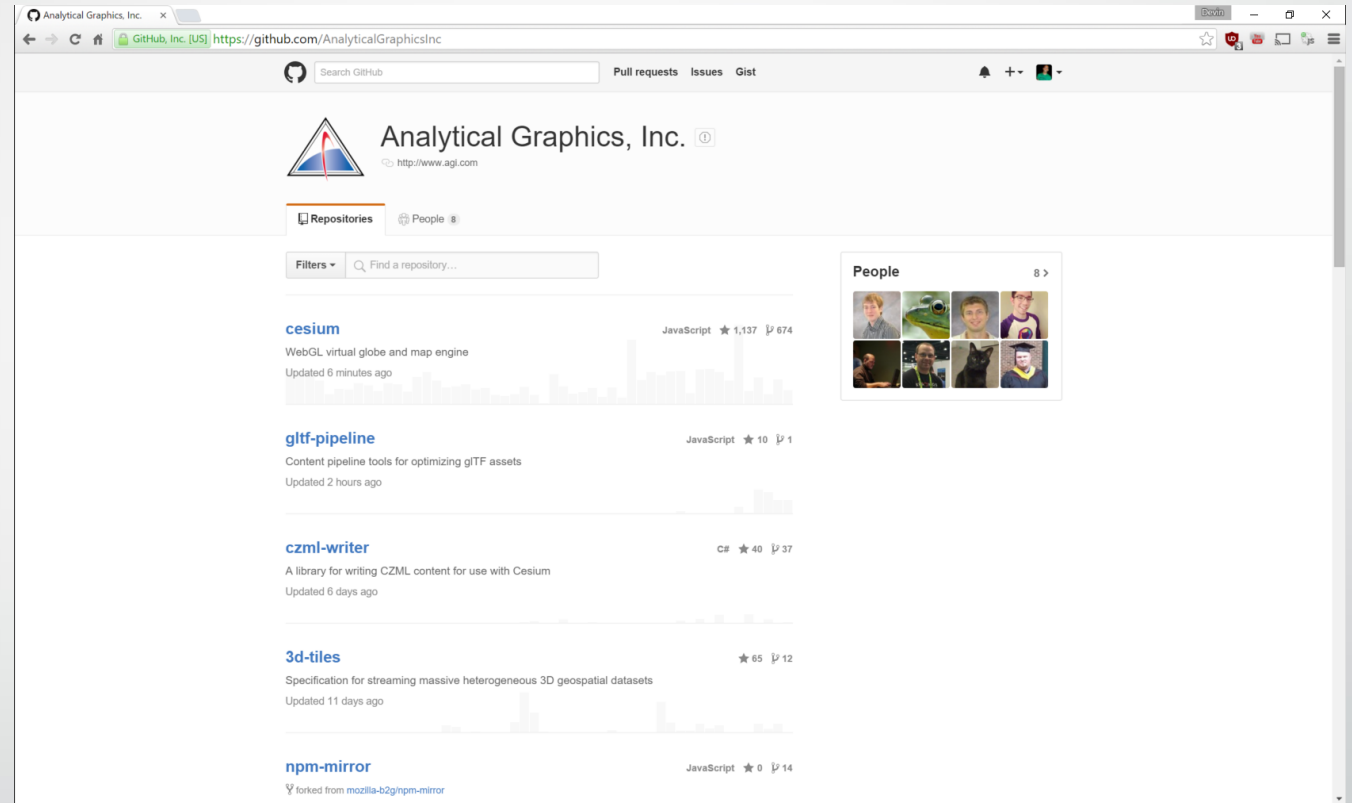
- They use another Amazon Cloud EC2 instance for holding space data assets.

- NetRange: 174.129.0.0 - 174.129.255.255
- CIDR: 174.129.0.0/16
- NetName: AMAZON-EC2-5
- NetHandle: NET-174-129-0-0-1
- Parent: NET174 (NET-174-0-0-0-0)
- NetType: Direct Allocation
- OriginAS:
- Organization: Amazon.com, Inc. (AMAZO-4)
- RegDate: 2008-08-08
- Updated: 2014-09-03

Passive Penetration Results Forum Searching

Summary:

- They have multiple GitHub repositories that we can search for possible server-side misconfiguration leading to vulnerabilities we can exploit.



Passive Penetration Results Forum Searching

Summary:

- We can not use a search engine on their internal forum page since they have configured the site not to respond to web crawler.

Forum - AGI

<https://www.agi.com/agiforum/> Analytical Graphics ▼

A description for this result is not available because of this site's robots.txt – learn more.

Passive Penetration Results People Search

Recall from Wikipedia the current CEO is Paul Graziani.

- **Facebook Search Term:** *AGI OR "Analytical Graphics" "Paul Graziani" site:facebook.com*
- We find he attend Google Lunar xPrize in 2008.
- We also find he won Aviation Week, "for donating software licenses to educational institutions and encouraging students to pursue science, technology, engineering and math" ([Facebook](#))

Satellite Tool Kit

October 14, 2008 at 1:04am

facebook Sign Up

Email or Phone Password Log In

Keep me logged in Forgot your password?

Satellite Tool Kit

Satellite Tool Kit

Astrobotic is broadly applying Satellite Tool Kit as gold-standard software for design and optimization of our Tranquility Trek. The generosity of AGI's STK gift is only exceeded by their hospitality at last week's user conference. Thank you, AGI. Pictured left to right

are: Paul Graziani (President and CEO, AGI), Alastair Firth (CMU BS ECE '10), Jonathan Bidwell (CMU MS HCI), Dan Kane (former VP, AGI)

Google Lunar XPRIZE

Notes by Google Lunar XPRIZE

All Notes

Get Notes via RSS

Embed Post

<table style="width:auto;">

<tr>

<td>

</td>

</tr>


<td style="font-family:arial,sans-serif;font-size:10pt;">

AstroboticBlogPhotos</td>

</tr>

</table>

Share

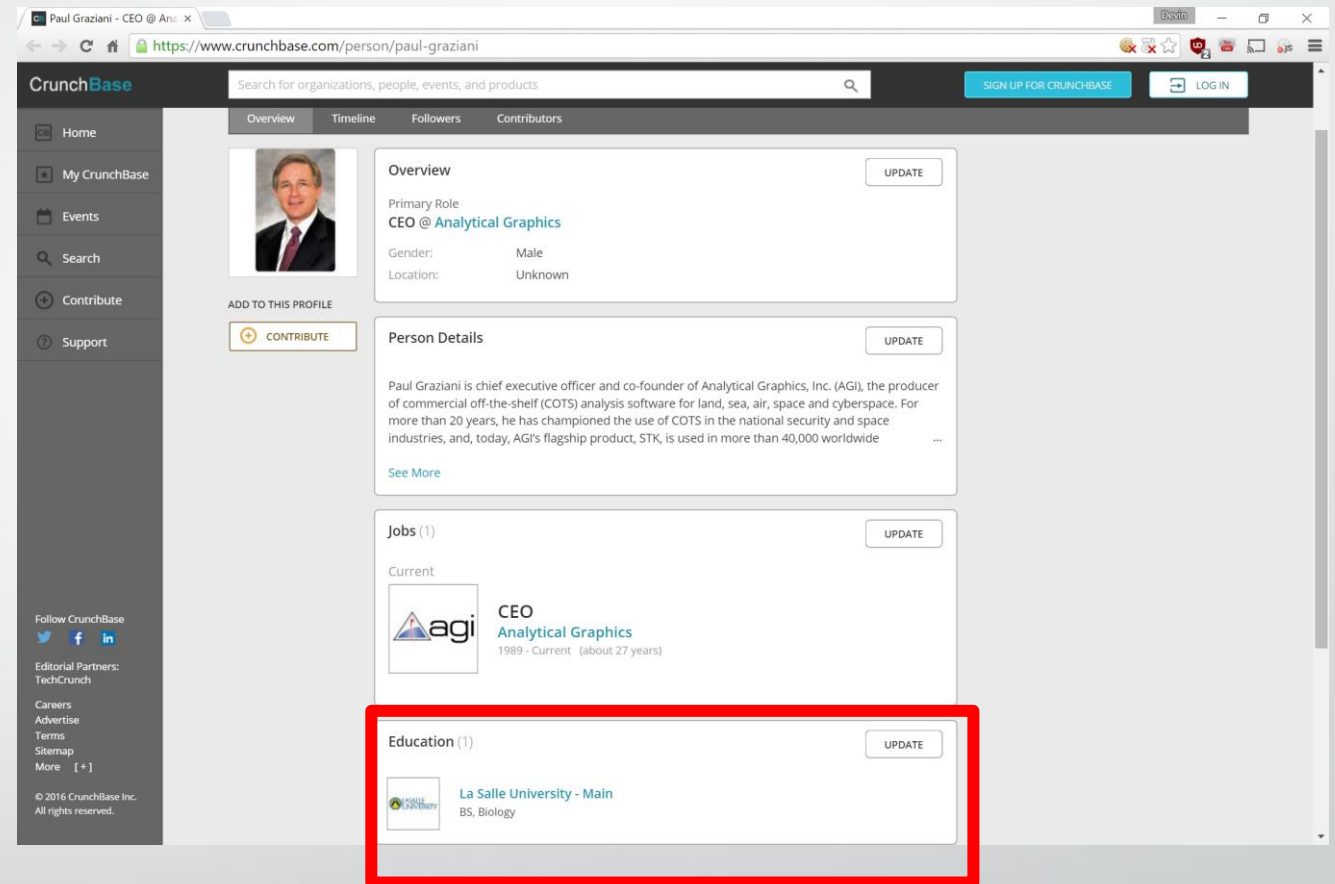


Passive Penetration Results People Search

Google Search Search Term: *AGI OR
"Analytical Graphics" "Paul Graziani" -agi.com*

- CrunchBase:
 - Attended La Salle University and obtained a BS in Biology

The Google results leads to him winning many other rewards.



The screenshot shows the CrunchBase profile for Paul Graziani, CEO of Analytical Graphics. The profile includes a header with navigation tabs (Overview, Timeline, Followers, Contributors), a profile picture, and a bio. The 'Overview' section lists his primary role as CEO at Analytical Graphics, gender as Male, and location as Unknown. The 'Person Details' section provides a brief biography of his career at AGI. The 'Jobs' section shows his current role as CEO of Analytical Graphics from 1989 to the present. The 'Education' section, highlighted with a red box, lists his education at La Salle University - Main, where he earned a BS in Biology.

CrunchBase

Search for organizations, people, events, and products

SIGN UP FOR CRUNCHBASE

LOG IN

Overview Timeline Followers Contributors

Home My CrunchBase Events Search Contribute Support

Follow CrunchBase

Editorial Partners: TechCrunch

Careers Advertise Terms Sitemap More [+]

© 2016 CrunchBase Inc. All rights reserved.

ADD TO THIS PROFILE

CONTRIBUTE

UPDATE

Overview

Primary Role
CEO @ Analytical Graphics

Gender: Male
Location: Unknown

Person Details

UPDATE

Paul Graziani is chief executive officer and co-founder of Analytical Graphics, Inc. (AGI), the producer of commercial off-the-shelf (COTS) analysis software for land, sea, air, space and cyberspace. For more than 20 years, he has championed the use of COTS in the national security and space industries, and, today, AGI's flagship product, STK, is used in more than 40,000 worldwide

See More

Jobs (1)

UPDATE

Current

agi CEO Analytical Graphics
1989 - Current (about 27 years)

Education (1)

UPDATE

La Salle University - Main
BS, Biology

Passive Penetration Results People Search

Recall from the Whois result:

Google Search Term: *"David Downs" AGI*
OR "Analytical Graphics" -agi.com

Spoke:

- Senior Network Administrator, Information Systems at Analytical Graphics Inc.

The screenshot shows a web browser window displaying a profile on the Spoke website. The browser's address bar shows the URL `www.spoke.com/info/p9ZXcLC/DavidDowns`. The page has a dark header with the Spoke logo and a search bar. Below the header, there's a navigation bar with tabs for SUMMARY, RESUME, BLOGS, ACHIEVEMENTS, LINKS, PEOPLE, and VIDEOS. The main content area is divided into several sections: a profile picture placeholder, a bio section with the name "David Downs" and title "Senior Network Administrator, Information Systems, Analytical Graphics Inc.", a contact section with fields for Telephone, Email, Background Report, and Public Records, and a digital info section with social media links for LinkedIn, Facebook, Google+, and Twitter. On the right side, there are additional sections: "See something that needs to be Updated?" with an "EDIT THIS PAGE" button, "Didn't find what you were looking for?" with a "FIND DAVID DOWNS" button, "PAGE COMPLETION" showing a 10% progress bar and options to "Add a Social Network", "Add an Industry", and "Add Education", and "PUBLIC RECORDS" with a link to "More on Archives".

Passive Penetration Results People Search

Recall from the Harvester Results a list of emails.

First email: tcarrico@agi.com

- **Google Search Term:** "*tcarrico*" AGI OR "*Analytical Graphics*" -agi.com
- We find his full name to be "Tim Carrico" – Business Development and Principle Software Engineer at AGI

Tim Carrico | Vizualize.me

vizualize.me/tcarrico

Dir Business Development/Principal SW Engineer at **AGI**. Created with Raphaël
EMPLOYMENT & EDUCATION '83 '84 '85 '86 '87 '88 '89 '90 '91 '92 '93 '94 '95 ...

Passive Penetration Results People Search

- No Facebook
- Does have a LinkedIn page but we can not browse anonymously thanks again to robots.txt

Tim Carrico | LinkedIn

<https://www.linkedin.com/in/tim-carrico-4600987>

Greater Boston Area - Applied Technology Leader, Innovator. - AGI

View **Tim Carrico's** professional profile on LinkedIn. ... typically revolved around difficult technical matters that we wanted to model in STK (one of **AGI's** products).

Passive Penetration Results People Search

Recall from the Harvester Results a list of emails.

Second email: *mglenn@agi.com*

Google Search Term: "*mglenn@agi.com*"

- We find his full name to be "Matt Glenn" – Manager of International Operations.

From: Glenn, Matt [<mailto:mglenn@agi.com>]
Sent: Thursday, January 31, 2013 2:47 PM
To: DDTC Response Team
Cc: 'Jon Roberts (JRoberts@MARBURLAW.COM)'
Subject: ITAR Amendment - Category IV

Dear DDTC Response Team,

Regarding 78 FR 6765-69, the proposed revision of USML Category IV continues use of the term "directly related to" in paragraph (i) Technical data. From my company's perspective there is ambiguity as to whether or not desktop trajectory modeling and simulation software currently controlled under Category IV(i) would still be ITAR-controlled under the proposed rule if enacted, even though the software does not meet the definition of "specially designed" as provided by the Department of State in the June 19, 2012 proposed rule (77 FR 36428).

We would be grateful for clarification, as we believe it could reduce future workload associated with product-specific commodity jurisdiction requests by industry, wherein assertions are built, presented and then debated, that this type of software is not "directly related to" the defense articles enumerated in paragraphs (a) through (h).

Thank you very much for your consideration.

Sincerely,

Matt Glenn
Manager, International Operations
Analytical Graphics, Inc.
220 Valley Creek Blvd.
Exton, PA 19341 USA
Tel: +1 (610) 981-8053
Fax: +1 (610) 981-8001



A Quick Active? Information Gathering Result

Monitor the traffic between our desktop and their web-server.

A Quick Active? Information Gathering Result

"pof -i eth0"

- Pof - "utilizes an array of sophisticated, purely passive traffic fingerprinting mechanisms to identify the players behind any incidental TCP/IP communications)" (coredump.cx)
- Shown is our client computer first contacting the server.

```
root@kali:~# pof -i eth0
[- pof 3.07b by Michal Zalewski <lcantuf@coredump.cx> ---
```

```
[+] Closed 1 file descriptor.
[+] Loaded 320 signatures from 'pof.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

```
-[ 192.168.73.141/49222 -> 65.89.176.31/80 (syn) ]-
```

```
client  = 192.168.73.141/49222
os      = Linux 3.11 and newer
dist    = 0
params  = none
raw_sig = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0
```

```
-[ 192.168.73.141/49222 -> 65.89.176.31/80 (mtu) ]-
```

```
client  = 192.168.73.141/49222
link    = Ethernet or modem
raw_mtu = 1500
```

```
----
```

```
-[ 192.168.73.141/49222 -> 65.89.176.31/80 (syn+ack) ]-
```

```
server  = 65.89.176.31/80
os      = Windows 7 or 8
dist    = 7
params  = tos:0x08
raw_sig = 4:121+7:0:1460:8192,8:mss,nop,ws,sok,ts:df,id+:0
```

```
----
```

```
-[ 192.168.73.141/49222 -> 65.89.176.31/80 (mtu) ]-
```

A Quick Active? Information Gathering Result

"pof-i etho"

- After starting the service we connect to the agi.com website to see if we can gather any useful information. We find that the destination server may be using Windows 7/8?
- We also see the server has been online for 23 days 4hrs and 28 mins.

```
-----
-[ 192.168.73.141/43296 -> 65.89.176.31/443 (uptime) ]-
client   = 192.168.73.141/43296
uptime   = 0 days 0 hrs 20 min (modulo 198 days)
raw_freq = 259.26 Hz
-----

-[ 192.168.73.141/43296 -> 65.89.176.31/443 (syn+ack) ]-
server   = 65.89.176.31/443
os        = Windows 7 or 8
dist      = 7
params    = tos:0x08
raw_sig   = 4:121+7:0:1460:8192,8:mss,nop,ws,sok,ts:df,id+:0
-----

-[ 192.168.73.141/43296 -> 65.89.176.31/443 (mtu) ]-
server   = 65.89.176.31/443
link      = Ethernet or modem
raw_mtu   = 1500
-----

-[ 192.168.73.141/43296 -> 65.89.176.31/443 (uptime) ]-
server   = 65.89.176.31/443
uptime   = 23 days 4 hrs 28 min (modulo 497 days)
raw_freq = 94.59 Hz
-----

-[ 192.168.73.141/57150 -> 208.111.135.82/80 (syn) ]-
-----
```

Concluding Summary



WIKIPEDIA
The Free Encyclopedia

- Wikipedia:
 - Offices in "Exton, Pennsylvania, [...] Washington, D.C., Colorado Springs, CO, Long Beach, CA, the UK and Singapore"
- The Harvester:
 - Company IP Space - 65.89.176.XXX
 - Their http service uses a SSL certificate.
 - They use Amazon cloud services. We can look over their GitHub to see if we can find any special keys that may be uploaded by accident.
 - A people search resulted in noting Paul Graziani as CEO, David Downs is the Senior Network Administrator, Tim Carrico as a Business Development and Principle Software Engineer at AGI, and Matt Glenn as a Manager of International Operation

Concluding Summary



- *pof-i etho:*
 - Their webserver probably is running a instance of Windows Server 2012.
 - Their web-server has been up for about 24days.