

## Challenges of Gathering Evidence from the Internet

Colin Ehren  
ACTWG Workshop  
June 11-13, 2013  
Santiago, Chile

Colin Ehren  
caren@gsa.gov  
Copyright C&SE 2013

---

---

---

---

---

---

---

---




## Overview

- Search Engines
- Invisible Web
- Social Media
- Compromise Issues & Internet Footprints
- Gathering & Evidencing content.

Colin Ehren  
caren@gsa.gov  
Copyright C&SE 2013

---

---

---



---

---

---

---

---

## Search Engines

**What does Google know?**

2007 - Eric Schmidt (Google CEO) estimated Google had indexed roughly 0.004% of the Internet.

July 2008 – Google had identified 1 trillion (1,000,000,000,000) unique URL's.

**Everything is on the Internet.**

It is estimated that 80% of Open Source information exists in Books, Magazines, Literature and other Media.

Colin Ehren  
caren@gsa.gov  
Copyright C&SE 2013

---

---

---

---

---

---

---

---




---

---

---

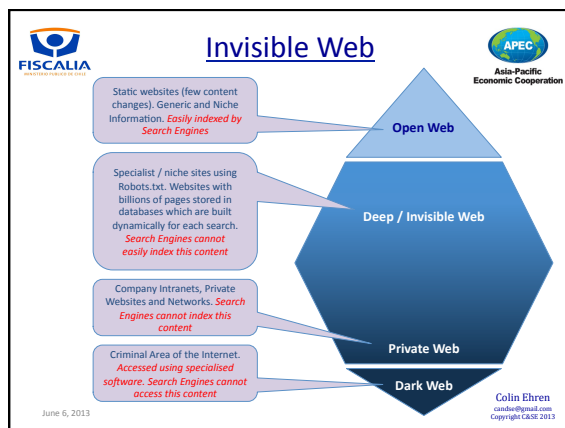
---

---

---

---

---




---

---

---

---

---

---

---

---

**Invisible Web**

July 2001, Michael Bergman produced a white paper for [www.brightplanet.com](http://www.brightplanet.com)

- 400 to 550 times larger than the World Wide Web.
- 7,500 terabytes of information compared to 19 terabytes on WWW.
- 550 billion documents compared to 30 billion on the WWW.
- 200,000+ deep Web sites.
- 60 of the largest sites collectively contained over 40x the information on the WWW.

2004 Study - identified 330,000+ Deep Web sites.  
Has grown almost exponentially since.

Colin Ehren  
csehn@msd.com  
Copyright C&SE 2013

---

---

---

---

---

---

---

---



### Social Media

- Austria, Belgium , Croatia, Cyprus, Czech Republic, Denmark, Finland, FYR of Macedonia, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Norway, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey & UK - Facebook, Youtube
- Bulgaria – Facebook, VBox7, Youtube
- Estonia – Facebook, Youtube, VKontakte
- France – Facebook, Skyrock, Youtube
- Hungary – Facebook, Iwiw, Youtube
- Latvia – Youtube, Draugiem, Facebook
- Lithuania – Facebook, Youtube, One
- Netherlands – Facebook, Hyves, Youtube
- Poland – Facebook, Youtube, Chomikuj
- Portugal – Facebook, Youtube, Twitter
- Romania – Facebook, Youtube, Hi5

June 6, 2013

Colin Ehren  
caren@msd.com  
Copyright C&SE 2013

---

---

---

---

---

---

---

---



### Social Media

- China.
  - Qzone, Tencent Weibo, Sina Weibo, RenRen
- Russia.
  - Vkontakte, Youtube, Odnoklassniki, Facebook, Livejournal
- India.
  - Facebook, Youtube, Orkut, Ibibo
- Georgia
  - Facebook, Youtube, Odnoklassniki, VKontakte
- Brazil
  - Facebook, Youtube, Twitter, Orkut
- Iran
  - Cloob, Facenama, Facebook?

June 6, 2013

Colin Ehren  
caren@msd.com  
Copyright C&SE 2013

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---



## Traditional Social Media Tools



Asia-Pacific  
Economic Cooperation

- Internet Relay Chat
- Usenet Talk Groups
- Google Groups / Yahoo Groups
- MSN/Skype, Yahoo, AOL Messengers and Chat Rooms
- E-mail
- Dedicated Discussion Forums
- Dating – Muslim Match, Uniform Match, Adult Friend
- Reunion Sites.

June 6, 2013

Colin Ehren  
csehren@gmail.com  
Copyright C&S 2013

---

---

---


---

---


---

---

---



## Compromise Issues



Asia-Pacific  
Economic Cooperation

Multiple ways to access the Internet;

- Corporate networked PC's
- Corporate stand-alone PC's
- Re-claimed stand-alone PC's
- Covert / Unattributed stand-alone PC's
- Covert / Unattributed networked PC's
- Working from Home (Stand-alone or Networked)
- Mobile Devices
- Internet Café's

June 6, 2013

Colin Ehren  
csehren@gmail.com  
Copyright C&S 2013

---

---

---


---

---


---

---

---



## Compromise Issues



Asia-Pacific  
Economic Cooperation

General Recommendation

All detailed or sensitive Internet research or Open Source Investigations should be undertaken on a covert or unattributed and registered PC, using a covert or unattributed Internet connection.

**Why?**

Your Internet Footprint could compromise yourself, your colleagues or an Investigation or Intelligence Operation that your Organisation or a Partner may be engaged in.

June 6, 2013

Colin Ehren  
csehren@gmail.com  
Copyright C&S 2013

---

---

---

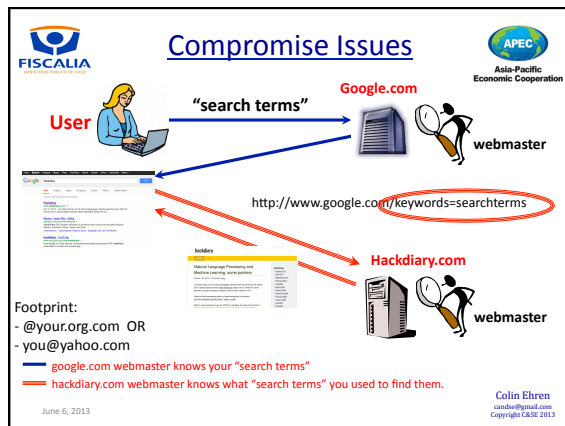
---

---

---

---

---




---

---

---

---

---

---

---

---

**Compromise Issues**

**FISCALIA** **APEC**  
Asia-Pacific Economic Cooperation

```

Browser: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0;
AWARELockDown2001; .NET CLR 1.1.4322)
Operating System: Windows 2000
Referer: http://www.google.co.uk/search?
q=am+i+secu+ch+sw+e+se+e+t=10&sa=N
Your IP Address: 195.173.172.10
IP Address Behind Firewall
Your hostname: mailgate.excitstrategy.co.uk
Your AS: 2529 AXIN ASN block
Your Country: GB
Your Abuse Contact: abuse@demon.net
Additional Software:
  
```

June 6, 2013

Colin Ehren  
csehren@gmail.com  
Copyright C&SE 2013

---

---

---

---

---

---

---

---

**Compromise Issues**

**FISCALIA** **APEC**  
Asia-Pacific Economic Cooperation

Home / Forums Index / Hardware and OS Related Technologies / Website Technology Issues

Forum Index > Chatting > Moderators: jasonst

**Website Technology Issues**

These terms have been highlighted:  
**awarelockdown2001** [ remove highlighting ]

**AWARELockDown2001**  
What user agent is that?

**dunne**

#: 672992

What user agent would "awarelockdown2001" be, anyone know? The host IP traces back to 1s4689-s0.metpolice.router.uk.quza.net, which is, ah, "interesting".

June 6, 2013

Colin Ehren  
csehren@gmail.com  
Copyright C&SE 2013

---

---

---


---

---


---


---

---



## Compromise Issues





Web Images Groups News Froogle more »

Search: "195.173.172.10" Search Advanced Search Preferences

Search: the web pages from the UK

**Web**

**METROPOLICE SERVICE**

195.173.172.10 resolved to mailgate.exitsstrategy.co.uk DNS Query Results: ; <>>  
[195.173.172.10](#) mailgate.exitsstrategy.co.uk ; global options: printcmd ...  
[www.fishers.ca/metropolice\\_service.htm](#) - 54k - [Cached](#) - [Similar pages](#)

[Usage Statistics www.wave.org - September 2003](#)  
4, 40, 2.31%, 31, 2.45%, 305, 3.91%, 4, 0.72%, **195.173.172.10** 5, 38, 2.19%, 0,  
0.00%, 8, 0.09%, 0, 0.00%, 66, 196.65 37 ...  
[www.wave.org/logs/usage\\_200309.html](#) - 107k - [Cached](#) - [Similar pages](#)

[MAKE EM LAUGH - Queen's Royal Hussars Bulletin Board](#)  
IP: **195.173.172.10** Gordon E Glazebrook Member. Posts: 345 From UK ... IP:  
**195.173.172.10** John Foster Member. Posts: 82 From Catterick North Yorkshire ...  
[bb.qth.org.uk/forum1/HTML000305-9.html](#) - 85k - [Cached](#) - [Similar pages](#)

**195.173.172.10**  
Unhappy/funny 0 0906/04 11:42 PM Re: I need some love. Hello! ... Lots  
and lots of hugs ... I'm so sorry you are feeling so lonely ...  
[www.helpforbs.com/messageboards/bbthreads/printthread.php?Board=livingroom&main=104211&type=post](#)

Colin Ehren  
cander@gmail.com  
Copyright © 2013

June 6, 2013

---

---

---

---

---

---

---

---

---

---



## Compromise Issues





Web Images Groups News Froogle more »

Search: "mailgate.exitsstrategy.co.uk" Search Advanced Search Preferences

Search: the web pages from the UK

**Web**

**METROPOLICE SERVICE**

195.173.172.10 resolved to mailgate.exitsstrategy.co.uk DNS Query Results: ; <>>  
DIG 9.2.2 <>> any mailgate.exitsstrategy.co.uk ; global options: printcmd ...  
[www.fishers.ca/metropolice\\_service.htm](#) - 54k - [Cached](#) - [Similar pages](#)

[UK screen - Page Statistics for HOPCYN BEO](#)  
... mailgate.exitsstrategy.co.uk, 22053, http://www.google.co.uk/search?hl=en&lr=&cm=country/UK/CCoun... UK crawler@googletbot.com, 1903, US ...  
[www.ukscreen.com/cast/hopcy/vstats](#) - 24k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)

[eXTReme Tracking](#)  
11 Nov, Fri, 14:31:05, mailgate.exitsstrategy.co.uk, MSIE 6, Windows 2000, 11 Nov,  
Fri, 14:30:45, ip:85-134-195-23 del.scribble.se, MSIE 6, Windows 95  
[extremetracking.com/open/unique?tag=whg92](#) - 51k - [Cached](#) - [Similar pages](#)

[eXTReme Tracking](#)  
... 08 Mar, Mon, 05:54:16, 195.173.14.60, MSIE 5, Windows NT, 08 Mar, Mon, 06:01:31,  
mailgate.exitsstrategy.co.uk, MSIE 5, Windows 2000, Last 20 Days, Unique Visitors ...  
[extremetracking.com/open/unique?tag=neurolog](#) - 51k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)

Colin Ehren  
cander@gmail.com  
Copyright © 2013

June 6, 2013

---

---

---

---

---


---

---


---

---

---



## Compromise Issues



**Network Whois record**

Queried whois.rpsa.net with "6 195.173.172.10" ...

195.173.172.0 - 195.173.172.15  
**METROPOLICE**  
Metropolitan Police Service  
London, ENGL  
ENGL

Colin Ehren  
cander@gmail.com  
Copyright © 2013

June 6, 2013

---

---

---

---

---



---

---

---

---


---



### Compromise Issues

**The “parallel surfing” Problem...**

- User #1: leaves “your.org” footprints whilst visiting “target.com”
- User #2: leaves “Covert” footprints whilst visiting “target.com”



The “Covert” User may now be recognized as an “your.org” visitor.

Colin Ehren  
candee@gmail.com  
Copyright C&SE 2013

---

---

---



---

---

---

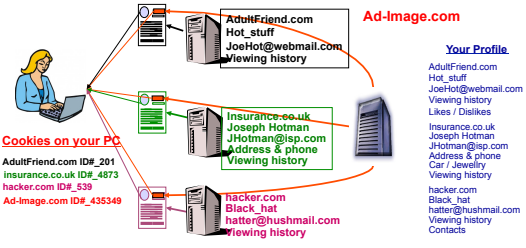
---

---



### Compromise Issues

Web pages can include images or adverts from third parties.



Companies, such as “Ad-Image.com” are able to compile a significant profile on you and your surfing habits, which they are able to trade or sell to their partners or customers.

Colin Ehren  
candee@gmail.com  
Copyright C&SE 2013

---

---

---



---

---

---

---

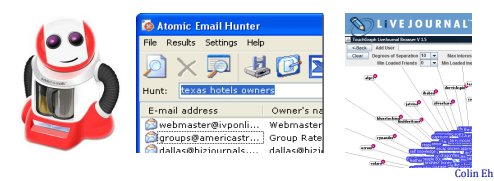
---



### Gathering Data

**Common Issue – Large amounts of data**

- Social Media Tools
- Data Extraction Tools.
- Visualisation Tools



Colin Ehren  
candee@gmail.com  
Copyright C&SE 2013

---

---

---

---

---

---

---

---



## Gathering Data





**CutePDF™** ideas for PDF



**Abduction!**  
3.0.18




June 7, 2013

Colin Ehren  
csehn@msd.com  
Copyright C&SE 2013

---

---

---


---

---


---

---

---

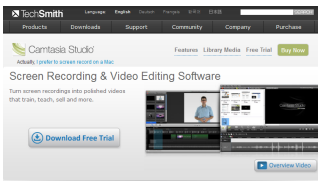


## Evidencing Data



Prove it or Lose it

All your efforts will be wasted unless you can prove what you found.



June 7, 2013

Colin Ehren  
csehn@msd.com  
Copyright C&SE 2013

---

---

---


---

---


---

---

---



## Evidencing Data



Preserving the Evidential Chain

When saving and moving Data the Investigator must ensure the Evidential Chain is preserved.

- This is done with the aid of an **MDS Hash Extractor**
  - A note is made of every number generated in relation to the files saved.
  - The Files are then copied to a CD/DVD Disk, and the Disk 'finalised' so that the files cannot be added to or deleted.
  - Then each file on the CD/DVD Disk is checked with the MDS Hash Extractor again, and the resulting numbers noted.
  - The resulting numbers generated should be identical.

The CD/DVD disk should now be sealed in an Evidential Envelope or Bag, or placed in an envelope and sealed with an adhesive Exhibit / Evidence Label.

June 7, 2013

Colin Ehren  
csehn@msd.com  
Copyright C&SE 2013

---

---

---

---



---

---

---

---





Asia-Pacific  
Economic Cooperation

## Challenges of Gathering Evidence from the Internet

Colin Ehren  
+44-7941-338449  
candse@gmail.com

Colin Ehren  
candse@gmail.com  
Copyright © 2013

---

---

---

---

---

---

---