

Chapter 48: Net:Geography Fieldwork Frequently Asked Questions

MARTIN DODGE* AND ROB KITCHIN†

*Centre for Advanced Spatial Analysis, University College London, London, U.K.; †NIRSA, National University of Ireland, Maynooth, Ireland

1. INTRODUCING THE NET:GEOGRAPHY FIELDWORK FAQ

Q. *What is the Net:Geography FAQ about?*

A. It is a set of answers to frequently asked questions (FAQs) regarding the geography and unseen, “inner”, structures of the Internet. It provides a practical “fieldwork” guide for understanding the Internet, using online mapping resources as virtual learning tools.

- It gives hands-on suggestions of techniques and freely available software tools and Web resources that can be used to actively explore both the internal topology of Internet connections and the external geography of network infrastructure. By revealing the operation of the Internet in terms of where things are located, who owns them, and how data travels, the FAQ helps foster a more critical engagement with the media. The goal is to contribute, in a small way, to changing users of the Internet from passive consumers to more informed and active citizens of their network, and potentially more engaged learners.
- It is possible to learn a lot about the Internet from critical writing, popular discourses, and secondary published data. However, for real understanding, there is no substitute for doing your own fieldwork.
- It is not necessary to be a network engineer or computer scientist to begin to ask critical questions about the structure and the operation of the Internet. Nor does not require a large investment in expensive, specialized tools as the Internet can be used to measure and map itself. Many of the tools and techniques used were actually created by engineers for practical purposes of “debugging” network problems. However, they can also be re-used in politically challenging ways in the context of virtual learning, providing tactical knowledge of the media that cannot be gained in any other way. As a consequence, anybody can do Net:Geography fieldwork.
- The practical examples given in this FAQ were tested using a standard PC running Windows 2000 on a university network, but most of the software tools and all of the techniques discussed are sufficiently generic that they should work in most situations.

- The Net:Geography FAQ comprises four sections: (1) finding out about your place on the Internet, (2) determining the location of components of the Internet, (3) measuring distance across the Internet, (4) charting the routes of data through the Internet.

Q. *In what ways is Net:Geography relevant to virtual learning environments (VLE)?*

A. The concept of doing “fieldwork” is very relevant to some of the underlying goals of VLEs—fostering active participation, developing social interaction by engaged learners, and mixing together learning resources and teaching approaches. Further, we would argue that specific Net:Geography methods outlined in this FAQ can contribute valuably to VLE development on three levels:

- Firstly, the practical techniques of network explorations and mapping can be incorporated as pedagogic content in a range of VLEs, particularly those that aim to explain “how the Internet works”.
- Secondly, the techniques are useful for academics and learners to look at and probe the underlying infrastructures that make their existing VLEs work.
- Lastly, the techniques can be used as part of thorough appraisal and assessment of the value of a VLE. Most obviously this can be achieved through monitoring online interactions and mapping the geography of participants.

Q. *Can I really explore the “inner workings” of the Internet without permission?*

A. Yes, even as an “ordinary user” you can begin to explore the structure and operation of the Internet. This is because the Internet is built and operated in a fundamentally different way to other large communication networks, like telephones or television. These other networks are purposefully closed and proprietary, and, unlike the Internet, actively try to keep “consumers” away from the insides of the network.

- The Internet was purposefully designed as an open network that encourages active exploration and experimentation. The Internet is not a single physical entity, instead it is premised on a public agreement to share data using open protocols. Anyone can use these protocols and as long as users abide by the terms of any access agreement and follow the protocols, they are able to take an active role in producing the network. Many of the most useful Internet services widely used today came about through researchers, students, and enthusiastic hackers exploring and exploiting this open architecture to try out new things.
- However, the openness of the Internet is always under attack because it is seen as threatening and subversive by many entrenched institutions. Today, with increasing commercial pressures, fears of criminal hackers,

rising levels of spam, viruses and worms, there is a definite “chilling effect” across the Net as security is tightened and the media comes under more surveillance.

- For a lucid discussion on the open design of the Internet, see Searls and Weinberger (2003).

Q. *Does the Internet actually have a geography?*

A. Yes it does. In fact, there are several different geographies, although this FAQ focuses on the material geography of the infrastructures of the Internet. Other important geographies that can be analyzed include, for example, the social geography of e-mail and the economic geography of content production and distribution.

- The hype around much of the “impact” of the Internet, especially in the mid-1990s, was that it was “everywhere and nowhere” and it would make geography less significant in human organization through the “death of distance”. This has patently not been the case.
- While the Internet has undoubtedly had an affect on the geography of business operation and the time–space patterns of individual communication and consumption, distance is not dead. What is being witnessed are complicated socio-economic restructurings, through processes of concentration and decentralization, across scales.
- The idea of the Internet as being somehow “anti-geographical” is based on three key notions: fantasy, denial, and ignorance
 1. Internet geography was assumed not to materially exist. This is founded on the anti-corporeal, cyber-utopianist *fantasy* that somehow the virtual communities of cyberspace can be produced in a realm divorced from material existence.
 2. Internet geography was assumed not to be important, so could be *denied*. The failure of many e-commerce ventures in the dotcom boom, we would argue, was based in part on ignoring the grounded, geographic, realities of computer-mediated communication, logistic networks, and labor markets.
 3. Internet geography was assumed to be not measurable. Because it was hard to do, it was *ignored*, especially in the heady days of bubble growth.
- The medium of communication might be virtual, but the Internet is dependent on physical infrastructure and human labor, most of which is invisible to users. The computers are small in scale and are usually hidden from view in anonymous server rooms and secure, windowless buildings, while the cables are under floors, in ceilings and in conduits buried under roads.
- The banal technicalities of Internet infrastructures are easily overlooked (just like for other essential utilities of water, electricity), but they are not naturally given. The geographical structure and operation

of networks that service modern living have politics. Net:Geography fieldwork can help you grasp some of these grounded politics first hand.

Q. *Why is understanding the geography of the Internet useful?*

A. There are several pragmatic reasons why being able to find out about the geographical structure of the Internet is useful. Most importantly, the Internet is a global system, but it is always a locally produced. Understanding the local variability enhances the understanding of the whole system.

- The social production of the Internet is contingent on cultural, legal, and economic forces that vary from place to place. In communicating with people, it is often useful to be sensitive to language, customs and time-zones differences for example.
- The production of the Internet is subject to myriad of different legal systems, which vary by territorial geography. It can be important to know the legal jurisdiction where the user is located as this may impact the types of consumer protection enjoyed, the particular obscenity laws enforced, and so on.
- The freedom to surf the Web is not universal. Governments in many countries try to impose varying degrees of censorship in the production and the consumption of information of their citizens. For an authoritative catalog of government's censorship efforts across the world, see Reporters without Borders (2003).
- In economic terms, Internet availability (as measured by access speeds, reliability, and cost) remains uneven across space and across different social groups. This has been characterized, often overly simplistically, as the "digital divide" and, for a nuanced analysis, it must be considered geographically.
- Knowing where things are located is also useful analytically because variations in spatial patterns can often give researchers an insight into underlying processes. Geographic location is one of the most effective means of indexing Internet data, enabling linkages to be made to a vast array of existing secondary data, such as demographic statistics from censuses and surveys. Geography also provides a familiar frame for presenting data about the Internet, giving context and additional meaning to numbers. Conventional geographic mapping remains one of the most powerful means of information presentation available (e.g., showing the locations of learners in a VLE).
- Lastly, in a world of evermore information and services on the Internet, geography proves to be an invaluable way of segmenting, filtering, and prioritizing people's attention. As a rule, people tend to be more interested in information that is local to them, rather than things that are distant.

2. FINDING OUT ABOUT YOUR PLACE ON THE INTERNET

We start the exploration of Net:Geography with some local fieldwork investigating how individuals are connected to the Internet, and what is happening in their local Internet neighborhood.

Q. *How am I connected to the Internet?*

A. You are connected to the Internet via specialist software and the settings that identify your location to the rest of the Internet. It is quite easy to find out these details using diagnostic utilities of the operating system to display the current Internet configuration for your PC.

- Technically these are the Transmission Control Protocol/Internet Protocol (TCP/IP) settings. TCP/IP is the basic lingua franca of the Internet. If your computer is connected to the Internet, it is “speaking” in TCP/IP.
- The ipconfig utility will show the TCP/IP settings. Run it by typing “*ipconfig/all*” from the command prompt. This gives the following type of output (Figure 1). (To open Command Prompt, click Start, then Programs, then Accessories.)
- The output looks technical (and it is to some extent) but all it shows is range of settings that allows the PC to get online. The most useful parts to note are the name of your PC on the Internet (*Host Name: mini-ferret*) and the *IP Address (128.40.59.54)*, which is the globally unique location of the PC in terms of the Internet’s internal topology. No other computer on the Internet can (legally) share the same address.

```
Command Prompt
C:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : MINI-FERRET
    Primary DNS Suffix . . . . . : casa.ucl.ac.uk
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : casa.ucl.ac.uk

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . : casa.ucl.ac.uk
    Description . . . . . : 3Com 3C920 Integrated Fast Ethernet
    Controller (3C905C-TX Compatible)
    Physical Address. . . . . : 00-06-5B-89-5A-9C
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 128.40.59.54
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 128.40.59.245
    DHCP Server . . . . . : 128.40.59.179
    DNS Servers . . . . . : 144.82.199.1
    . . . . . : 144.82.100.41
    Primary WINS Server . . . . . : 128.40.59.244
    Secondary WINS Server . . . . . : 128.40.58.142
    Lease Obtained. . . . . : 19 April 2004 18:28:53
    Lease Expires . . . . . : 21 April 2004 18:28:53

C:\>
```

Figure 1. TCP/IP settings reveal the structure of your local Net:Geography.

- Details are also given on the type of connection, in this case through a local area network using Ethernet, with the make and model of the card (*Description: 3Com 3C920*). The physical address of the card, a globally unique id code number that identifies this piece of hardware (*00-06-5B-89-5A-9C*) is also shown.
- Lastly, the output lists the IP addresses of the *Default Gateway* (*128.40.59.245*), which passes traffic from the local area out to the wider Internet, and the *DNS Servers* (*144.82.100.1 ; 144.82.100.41*), which are important components in the Internet for translating domain names into numeric IP addresses.

Q. *What is the speed of my connection?*

A. You can easily obtain the speed (and other useful statistics) on your current Internet connection.

- Open the Network and Dial-Up Connections menu (accessed from Start, Settings). Right click on the active network connection and select the *status* option (Figure 2).
- In this case the connection is running at *10 Mbps* (megabits per second). This is typical for an office environment and is quite a lot faster than average home, Internet access. Also displayed is the duration of the session and a basic indication of activity in terms of the total data transferred in and out.
- The speed of connection is important because it determines the bandwidth available for Internet interactions. Bandwidth is the capacity to shift data measured in bit per second and is crucial to what can be done

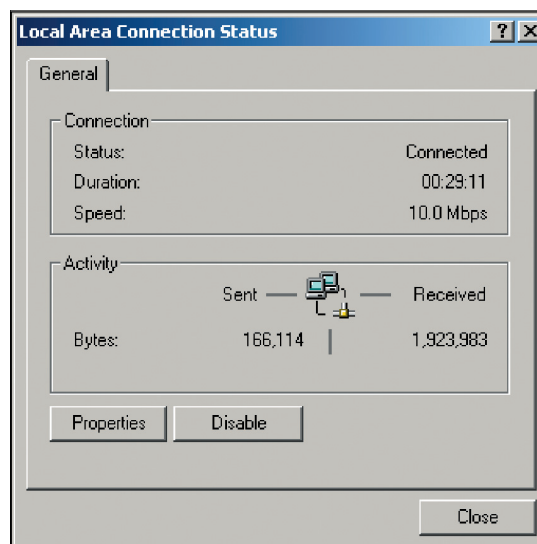


Figure 2. Network status showing the speed of connection.

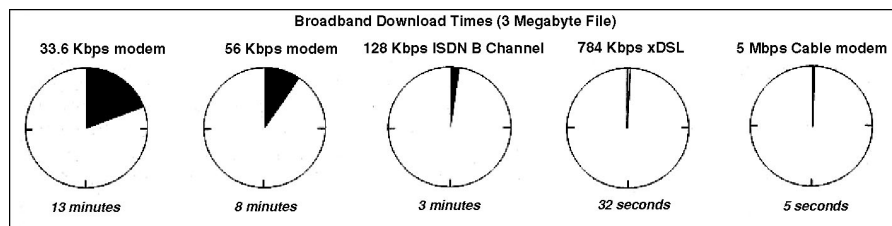


Figure 3. The importance of bandwidth.

and how long it will take, as illustrated by Figure 3. Some Internet services are simply not viable over low bandwidth connections.

Q. *What is going on in my local Internet neighborhood?*

A. It is possible to see in some detail the inner structure of a local part of the Internet, observing the activities of other users, using network monitoring tools.

- There are lots of different tools available. One of the most capable is the Ethereal Network Analyzer. It is a free, open-source application, downloadable from <http://www.ethereal.com>.
- Ethereal is a network monitoring tool that does “packet sniffing”. This means it can watch all the traffic “going past” your PC on a local network. This traffic is in the form of streams of individual data packets flowing between different machines. The data packets can be captured by Ethereal for processing and detailed analysis.
- Figure 4 shows Ethereal monitoring a small local area network of an office at a university. It was able to “sniff” quite a lot of activity nearby. This screenshot only shows a snapshot of a few seconds of the data packets flowing by the monitoring PC.
- The display looks complicated as it shows a very detailed view of Internet activity that most people never see. The result is simply a long list of all traffic “sniffed” rather than a summary graph or a map. Ethereal does not “know” anything about the physical structure of the network or the actual locations of the users. However, it is able to identify the different types traffic and, most importantly, the source and destination of the traffic.
- The top window in the Ethereal interface displays one data packet per line. It takes some care and skill to interpret what is going in terms of user activity because it can be fragmented over many individual data packets. As an example, one data packet, number 2449, has been selected. The data was sent from PC identified as *casa198.bart.ucl.ac.uk* (Source column) to *newswww.bbc.net.uk* (Destination column). The destination is the Web server for the BBC News service. The protocol of the data packet was *http* (hypertext transfer protocol used by Web browsers) and

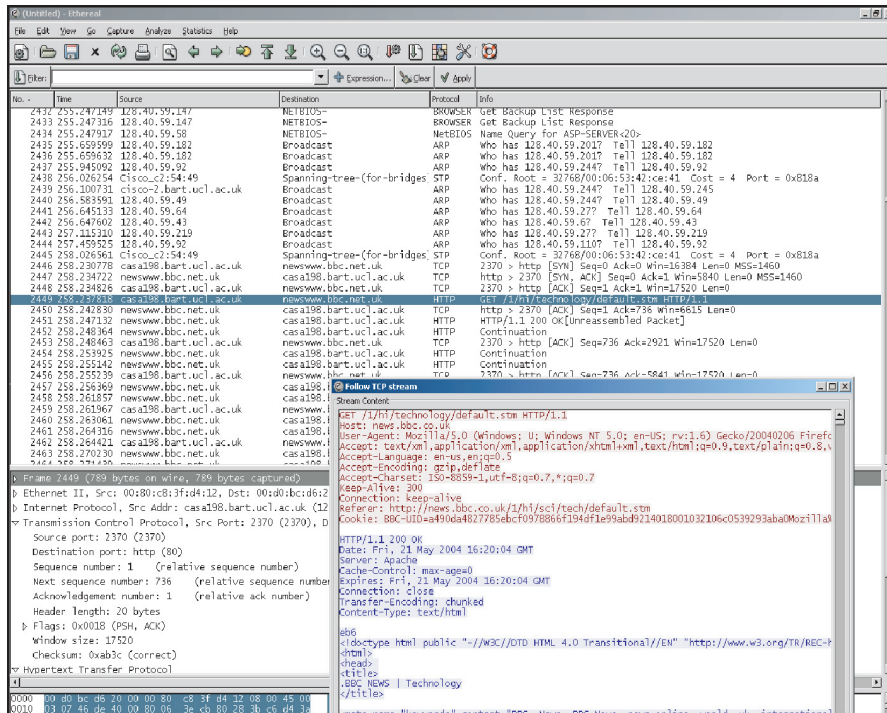


Figure 4. Ethereal Network Analyzer capturing packet-level detail on the traffic flows of a local network environment.

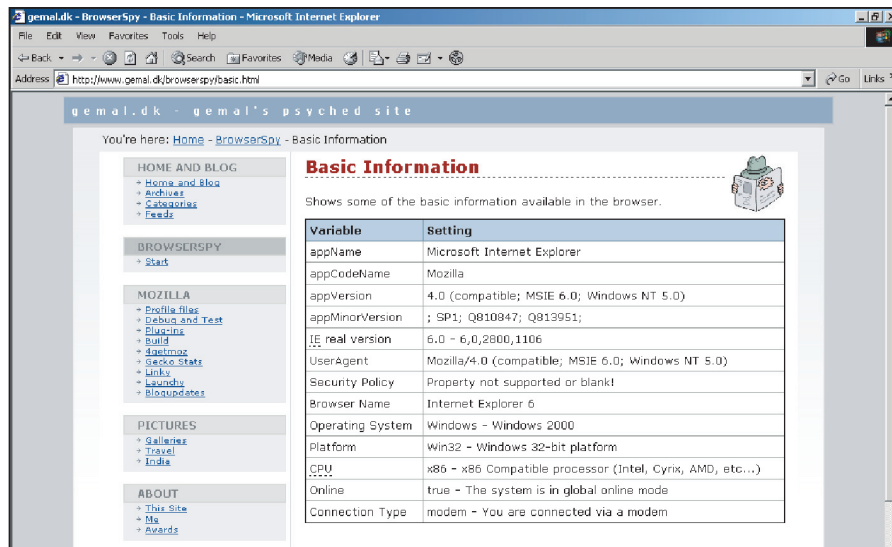
the *GET* command Info column reveals it was a request for a Web page. Ethereal can connect together all the related packets of data for this particular Web transaction, shown in the “Follow TCP Stream” pop-up window, enabling us to see the actual Web page content (in raw html form). In this case Ethereal was able to show exactly the Web page this user was looking at.

- Ethereal, and similar network monitoring tools, have the power to reveal a great deal about individual user’s activities. This is particularly so because most data flowing across the Internet are sent unencrypted and can be covertly read by anyone who is able to tap into the network flow.
- Beyond the practicalities of running network monitoring tools like Ethereal and interpreting the output, there are clearly some more thorny ethical issues to confront about covert “spying” on the activities of your neighbors. Good ethical practice for researchers would require that prior informed consent is obtained from *all* people on the network being scanned. Active network scanning for benign Net:Geography exploration can also be deemed improper behavior by system administrators, so you need to be prepared to justify your actions.

Q. *What do I reveal about myself to the rest of the Internet?*

A. Connecting to the Internet means necessarily revealing some details to network providers and leaving traces in the logs of the services you interact with. At a most basic level the IP address must be known to send data to the correct location.

- Any online activity leave traces, but using different services and different client software results in different amounts of potentially personally identifiable data “leaking” out.
- Surfing the Web in particular results in a considerable amount of information being revealed. Even if you have not formally registered with websites and feel that you are browsing anonymously, you may be surprised the degree to which you are trackable.
- There are number of free Web services that test what is revealed about your PC and Web browser configuration. Figure 5 shows an example produced by the BrowserSpy service (<http://gemal.dk/browserspy>).
- The “basic information” that BrowserSpy is able to extract is perhaps not that surprising it can determine the type of Web browser and version, as well as the operating system. More interestingly it could tell the connection was via a modem. BrowserSpy is also able to gather many more details from a typical Web browser (e.g., plug-ins available, drive letters, screen resolution, time-zone settings). In many ways this is technical and very banal information, but taken together this voluntary “leakage” can paint a detailed picture of your PC. These data are useful for websites in building profiles and tracking their users,



The screenshot shows a Microsoft Internet Explorer window with the address bar set to <http://www.gemal.dk/browserspy/basic.html>. The page content includes a navigation menu on the left and a main section titled "Basic Information" which contains a table of browser and system details.

Variable	Setting
appName	Microsoft Internet Explorer
appCodeName	Mozilla
appVersion	4.0 (compatible; MSIE 6.0; Windows NT 5.0)
appMinorVersion	; SP1; Q810847; Q813951;
IE real version	6.0 - 6.0.2600.1106
UserAgent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Security Policy	Property not supported or blank!
Browser Name	Internet Explorer 6
Operating System	Windows - Windows 2000
Platform	win32 - Windows 32-bit platform
CPU	x86 - x86 Compatible processor (Intel, Cyrix, AMD, etc...)
Online	true - The system is in global online mode
Connection Type	modem - You are connected via a modem

Figure 5. An example of some of the possible “hidden” details that you can unwittingly reveal to websites.

and also for automatically presenting tailored content to suit different users (e.g., less graphics for those on low bandwidth connections). It can also be exploited by more unscrupulous people to identify potential vulnerabilities in your PC through which to attempt to break in.

- Browser cookies are particularly pernicious tool in Web surveillance, although we do not have space to discuss their role in actively tracking individual browsing patterns. However, as a very simple test of their prevalence, try setting your browser so that it has to request permission from you every time a website wants to set a cookie. You will quickly see just how many are set!
- Further technical reading on what data are known about you when using the Internet see Clayton (2001).

3. LOCATION ON THE INTERNET

We now look beyond the local neighborhood to methods that allow a wider exploration of where things are located on the Internet.

Q. *How is location in the Internet defined?*

A. Knowing where things are located is crucial to most activities, including in the Internet. However, the Internet is concerned with topological location (the where things are located in terms of connections) and not with physical geographical location, defined by x, y co-ordinates.

- The Internet comprises a robust and scaleable system to specify location uniquely so that data can be correctly transferred.
- As demonstrated earlier when discussing *ipconfig*, globally unique locations in the Internet are based on two key systems—IP addresses and domain names.
- Typically when people give out an Internet location this will be some kind of domain name address (e.g., a website address, *http://www.jasonnolan.net* or an e-mail address such as *jason.nolan@utoronto.ca*). Domain names are always associated with an IP address.
- IP addresses are little seen or used by typical users. They look a little like telephone numbers, such as *64.246.60.38*, identifying the *http://www.jasonnolan.net* website. The unique allocation of IP addresses is the key to the successful delivery of traffic across the complexity of the global Internet.

Q. *Why don't Internet addresses specify a geographic position?*

A. This is how they were designed. Basically, the Internet protocols at the core of the network were never designed to make details on its geographical structure explicit to users. The successful transfer of data through the Internet requires knowledge of a topological address, not geographical location.

- In many ways the Internet was designed to deliberately hide the underlying physical geography. This split between logical locations and physical locations is actually very useful. It is part of the reason why you can surf across websites scattered across the world and not have to worry about where the data are physically located.
- Because the Internet is a network of networks, rather than a homogeneous entity, its means of control are decentralized and its structure is fluid. Even though “no one owns the Internet” as a whole, each one of its component parts is owned and operated by many millions of different organizations and individuals. In consequence, no one single institution has a synoptic view of the whole Internet and, therefore, no one is required to maintain a register of where all the components are physically located.
- However, it is often useful to be able to determine the geographic location of parts of the Internet, for example the location of a website as a part of assessment of whether they are credible sources of information or before entering credit card details. Many websites might not be physically where you think they are. However, because there is no one central register to do this mapping, you have to use a range of different fieldwork techniques need to be used (detailed below).

Q. *What types of geographic location are relevant for Net:Geography fieldwork?*

A. Understanding the nature of the geographical location of components of the Internet is interesting because different parts can be in different places. There are five obvious kinds of geographical location which are important in terms of the Web:

1. A website is where it is published that is where the server is physically located (hardware geography).
2. A website is where the author/maintainer is located (production geography).
3. A website is where the legal owner is located (ownership geography).
4. A website is where the readers are located (audience geography).
5. A website is where the content refers (lexical geography).
 - In some cases all five locations will be coincident. But it is easy to imagine plausible scenarios in which you have a Web page about Maynooth, Ireland that is written by someone in Canada, hosted on a server in London and read by people from across the world.
 - The geographical precision of these different physical locations can also vary. Sometimes location might be determined as the precise x, y position (e.g., street address of the building with the Web server) other times one might only know city or legal jurisdiction referred to.

Q. *How can I tell where an Internet address is geographically located?*

A. Unfortunately, determining the precise geographic location of an Internet address cannot be done easily or in an accurate, consistent fashion. However, there are some techniques that can be used to try to determine the geographic location, at least approximately, of a website for example.

- The first point to note is that different techniques will tell you about the five different locational types. Most of the techniques described here will identify the production or ownership geography.
- The first, and most obvious, method is to use lexical location as the proxy. Here, the content of the website is browsed to try to find an “about page” or “contacts page” that provides a postal address or telephone number of the owner. Other cultural and linguistic clues (e.g., flags, symbols) in the content of a website might give useful indications of the “real-world” location.
- If you only have the domain name of a website to work with, the first place to start is by “decoding” it. Many domain names are allocated on a country-by-country basis with their name ending with the appropriate two letter ISO country code (e.g., *.ca* for Canadian domains, *.ie* for Irish domains, and so on). One can infer the geographic location of an Internet address based on the country code in its domain name. A useful list of all the country code domain names is available at <http://www.iana.org/cctld/cctld-whois.htm>.
- However, there are limitations in relying on country code domains.
 1. There are several domain name types (the so called “global top-level domains”) that are not related to countries. The biggest of these are *.com*, *.org*, *.net* and *.info*. The <http://www.jasonnolan.net> website has a *.net* domain name which does not allow any inference on its location to be made. A *.net* domain could be located anywhere in the world. (Note, the top-level domains *.mil*, *.edu* and *.gov* are allocated only to U.S. institutions, so one can be fairly safely assume they are located in the U.S.A.)
 2. The level of geographic precision is obviously crude with this technique, particularly so for large countries. A *.ca* domain name could be anywhere in Canada.
 3. Lastly, just because a website uses a country code domain name does not guarantee that the website is actually within the country indicated. The ownership, production, hosting, and use of that website could well be in another country or several different countries. For example, the *amazon.de* and *amazon.co.uk* websites are published on servers physically located in the United States and not in the United Kingdom or Germany as indicated by their domain names.
- Moving beyond decoding the top-level domain names, you can try to exploit other parts of the domain name to infer geographic location of the address. This works when e-mail addresses or websites

are part of an established, easily identifiable company or institution that can be traced to city in which they are located. For example, we could deduce that Martin Dodge's e-mail address at ucl.ac.uk links him to University College London (UCL) and could then infer that he is physically located in central London, on the site of the main university campus. Again, there are limits to the level of precision in this method, and it is also prone to error for large organizations, like transnational companies, which operate from many sites, over extensive areas.

- The last thing you can do with a domain name address is to find out whom it is registered to. All domain names have a legal owner and the registration databases for this usually contain contact details. You can freely consult this registration information from the domain name system using a *Whois* query. (Note, not all domain registration databases will publicly give out the full address details of the owner.)
- A *Whois* query can be easily run from any number of websites. Below is the results of a *Whois* query to find the registered owner of *jasonnolan.net* domain name using the free service provided by AllWhois (<http://www.allwhois.com>) (Figure 6).

The screenshot shows the AllDomains.com website interface. At the top, there is a navigation menu with options: DOMAIN NAMES, ADDITIONAL SERVICES, TRANSFER DOMAINS, RESELLER ACCOUNTS, and CUSTOMER SUPPORT. Below the navigation, there is a section titled "About Allwhois" which explains the service. A search box contains the domain "www.jasonnolan.net" and a "Search" button. Below the search box, the "Whois Output:" section shows the search results for "jasonnolan.net". The results indicate that the domain is taken and provide the following contact information:

Registrant:
 KND1
 40 St George
 Suite 7224
 University of Toronto
 Toronto, Ontario M5S 2E4
 CA

Domain name: JASONNOLAN.NET

Administrative Contact:
 Nolan, Jason jason.nolan@utoronto.ca
 40 St George
 Suite 7224
 University of Toronto
 Toronto, Ontario M5S 2E4

There are also promotional banners for "DOMAINS.CN" and "POP3 EMAIL" visible on the page.

Figure 6. Looking up the domain name registrations details on *jasonnolan.net* using Whois.

- The registration information from the *Whois* query identifies the owner of *jasonnolan.net* to be located in Toronto, Canada. The full street address is given. This could be looked up and a detailed map obtained giving the precise location.
- The results of *Whois* queries can be very useful in finding out where the registered owner of a domain name is, however they are not always accurate. Firstly, registration details held on a given domain name may be out of date, incorrect, or deliberately false (spammers, for example, try to hide their true geographic location and would be unlikely to complete the registration honestly). Secondly, ownership details may only tell you one of the five possible geographies of a website. We can see that *jasonnolan.net*'s owner is located in Toronto, but the site may be produced, published, and consumed elsewhere. Thirdly, the registrations for large organizations often give a single postal address (their headquarters) and thereby mask where individual domain names are actually being used.
- If you do not have a domain name to work with, you can also lookup the ownership of IP addresses. These are generally allocated in large blocks to ISPs rather than to individuals or companies. You can do this query by doing a *Whois* query to ARIN (<http://www.arin.net/whois>). The IP address of the server which publishes <http://www.jasonnolan.net> is 64.246.60.38 (Figure 7). Looking up this address yields details on the registered owner, a company called Everyone's Internet Inc., with a postal address in Houston Texas.
- Another strategy is to test where a website is connected to the Internet by tracing traffic flows. Details on how to do this real-time probing are discussed in the last section of the FAQ.
- There are a number of firms that provide commercial services to convert IP addresses to geographic locations. For example, Quova, Inc. (<http://www.quova.com>), IP2Location (<http://www.ip2location.com>).
- To find out more on the technicalities of relating Internet addresses to geographic locations, see Lakhina et al. (2002) and Padmanabhan and Subramaniann (2001).

Q. *What else can I do to find out more about a website's ownership and location?*

A. Taking a different perspective, you can also explore the "virtual" position of a website in terms of its visibility in the information space of the Web.

- Counting the number of hyperlinks to and from a website and analyzing whom the links come from can reveal the informational structures of Net:Geography. The results can be used to infer a website's position in terms of social networks and power geometries; a well-linked site could indicate that its creator has power and influence. This kind of hyperlink analysis has many parallels to citation analysis used to assess influence in scholarly research. Much of the success of the Google search engine

Output from ARIN WHOIS

[ARIN Home Page](#)
[ARIN Site Map](#)
[ARIN WHOIS Help](#)
[Tutorial on Querying ARIN's WHOIS](#)

Search for :

Search results for: 64.246.60.38

```

OrgName:      Everyones Internet, Inc.
OrgID:        EVRY
Address:      2600 Southwest Freeway
Address:      Suite 500
City:         Houston
StateProv:   TX
PostalCode:  77098
Country:     US

NetRange:    64.246.0.0 - 64.246.63.255
CIDR:        64.246.0.0/18
NetName:     EVRY-BLK-9
NetHandle:   NET-64-246-0-0-1
Parent:      NET-64-0-0-0-0
NetType:     Direct Allocation
NameServer:  NS1.EV1.NET
NameServer:  NS2.EV1.NET
Comment:     ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:     2001-10-05
Updated:     2003-03-31

TechHandle:  RW172-ARIN
TechName:    Williams, Randy
TechPhone:   +1-713-400-5400

```

Figure 7. The results of a Whois lookup on the IP address of the Web server that hosts <http://www.jasonnolan.net>.

in terms of relevance ranking depends on its analysis of hyperlink structures to indicate the most credible sources of information.

- It is possible to obtain appropriate data to give a rough approximation of hyperlink structures using some of the large Web search engines. These will report link statistics (usually available as part of their advanced search options). For example using Google you can find out the number and origin of incoming hyperlinks made to the *jasonnolan.net* website using the search command *link: jasonnolan.net* (Figure 8).
- The Google search engine index reports 346 Web pages with hyperlinks to *http://www.jasonnolan.net*. This is a respectable number of links.

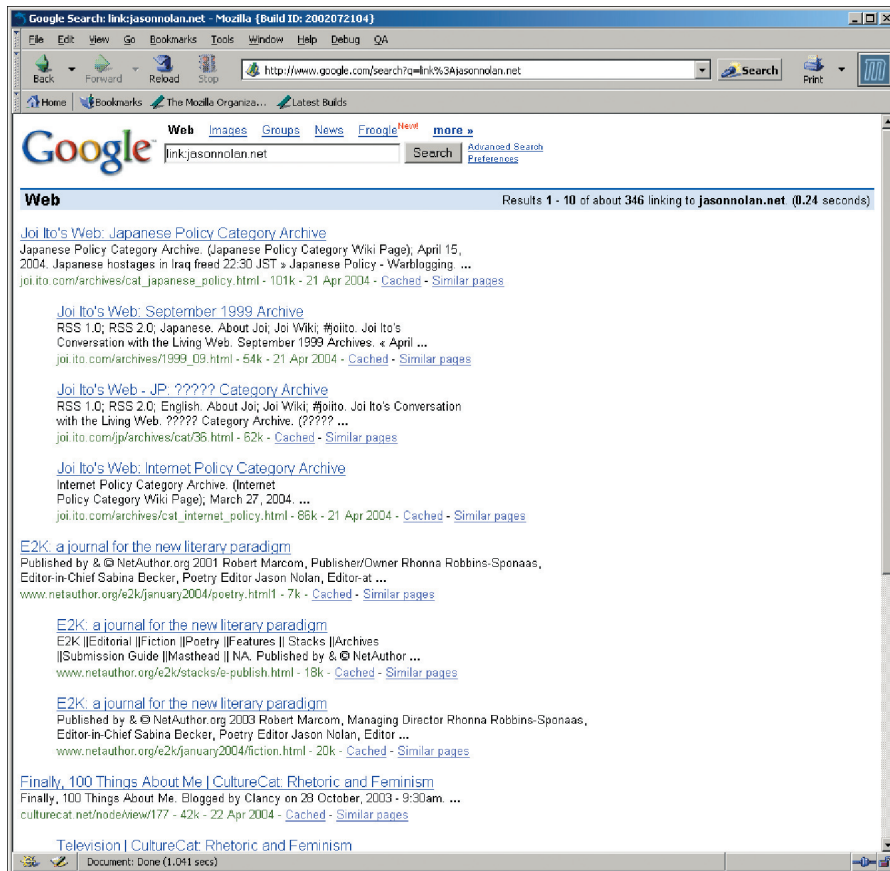


Figure 8. Incoming hyperlinks to <http://www.jasonnolan.net> website according to the Google index.

From a limited understanding, many of them appear to come from blogs citations. This is perhaps not surprising as [jasonnolan.net](http://www.jasonnolan.net) is also a blog.

- These types of informational structures can also be viewed as graphs, where the Web pages are nodes and the hyperlinks are connecting lines. A nice example of this is available using *GoogleBrowser*, an interactive tool produced by TouchGraph (<http://www.touchgraph.com>). It allows the active exploration of a website's location in terms of the virtual economy of linkages. Figure 9 shows an example of the *GoogleBrowser* view of linkage network immediately around <http://www.jasonnolan.net>.
- For those interested in exploiting the tactical power of hyperlink analysis to expose the hidden politics of Net:Geography, the research of Richard Rogers and colleagues is well worth consulting (<http://www.govcom.org>).

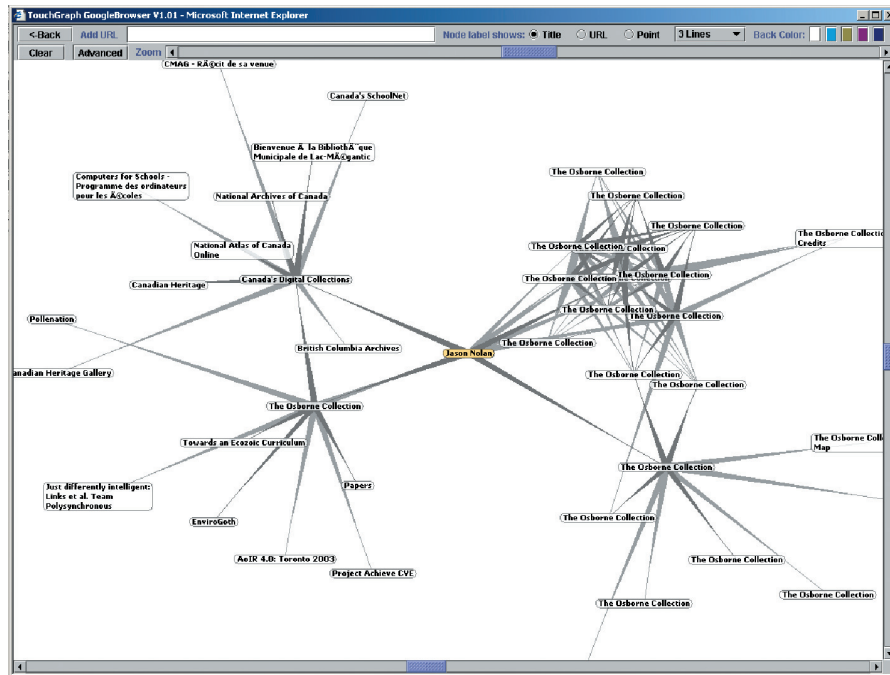


Figure 9. GoogleBrowser view of the local Web neighborhood of <http://www.jasonnolan.net>.

4. MEASURING DISTANCE ACROSS THE INTERNET

Q. How is distance across the Internet defined?

- A. Simply put, distance is measured in terms of time inside the Internet.
- Within the topological structure of the Internet, physical distances between places have little meaning or relevance. Instead relative distances are measured using the “journey” time taken to transmit and receive data.
 - This “journey” time is called latency. Increasing latency implies increasing relative distance between two places on the Internet. Latency metrics serve the same purpose as physical distance on road signs and maps, that is they tell you how “near” or “far” apart things are. It is important to note, however, that there can be many different technical factors (e.g., types of hardware and network configurations) that effect latency.
 - Of course time, and associated costs, are also widely used in the “real” world to express distance. Most people assess a journey in terms of the time it takes and not linear distance on the ground (e.g., a 10-minute drive to the shops, a 4-hour flight to a holiday destination). Time-based distance measures are useful to people because they match subjective perceptions of closeness, relevance, and importance. Near things tend

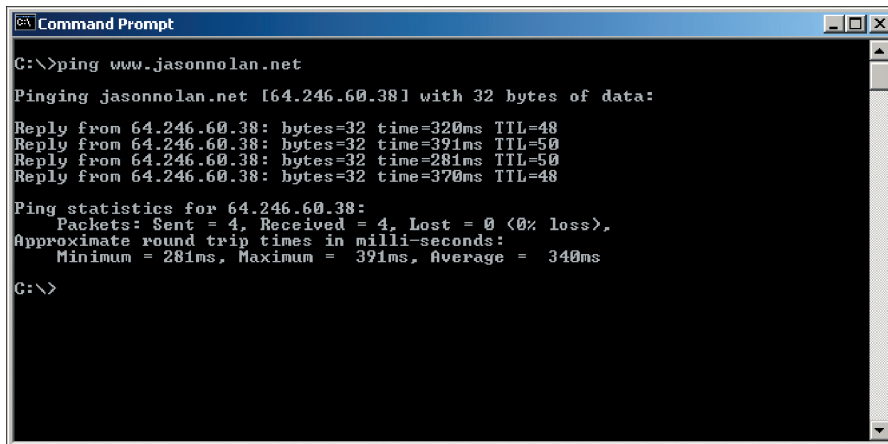
to be judged as more important because people's exposure to them is more direct, immediate, and frequent. Far away things take longer to experience and thus tend to be less familiar (e.g., people speak a different language) and are perceived as less comfortable and perhaps even as more risky.

- An interesting point of analysis, both on the Internet and in the “real” world, is to compute the relationship between distance on the ground and time distance for different places. This relationship is not always linear because of barriers, lack of connectivity, and poor accessibility. Sometimes the quickest places to reach are not always the closest physically. Analyzing the variable patterns in time accessibility can sometimes give insight into underlying structural processes.
- Distance can also be measured by the complexity of the journey, such as the number of interchanges encountered. In terms of the Internet, the least-complex distance would consist of the minimal number of different networks crossed or switching points negotiated, which may or may not be the same as the quickest route. The next section of the FAQ demonstrates how route complexity can be plotted by tracing traffic flows.

Q. *How can I actually measure latency?*

A. There is a useful utility called *ping* that can measure latency (the travel time of data) on the Internet. Ping is easy to use and available on most PCs.

- It is a network measurement tool primarily used by engineers to diagnose connectivity problems. Basically, it reports whether a particular place on the Internet is “live” and accepting data.
- Ping takes its name from the sound that submarine SONAR uses. Conceptually it works in a similar fashion by sending out small packets of test data to a target host and listening for a response. It is useful for distance measurement because it reports the round-trip time of data packets.
- Figure 10 shows an example of measuring the distance from a PC in London, U.K. to <http://www.jasonnolan.net> using ping.
- By default on Windows, ping sends out four test data packets. The time each took to go from London to <http://www.jasonnolan.net>'s server and back again is reported (in milliseconds). The last line of the output reports the overall statistics. According to this, the average “distance” for this particular journey across the Internet as measured by latency was 340 ms, while the slowest data packet took 391 ms.
- This type of time distance measurement is very susceptible to changes in conditions on the Internet, especially congestion in traffic flows. Internet distances measured by latency are never fixed. However, this



```
Command Prompt
C:\>ping www.jasonnolan.net
Pinging jasonnolan.net [64.246.60.38] with 32 bytes of data:
Reply from 64.246.60.38: bytes=32 time=320ms TTL=48
Reply from 64.246.60.38: bytes=32 time=391ms TTL=50
Reply from 64.246.60.38: bytes=32 time=281ms TTL=50
Reply from 64.246.60.38: bytes=32 time=370ms TTL=48
Ping statistics for 64.246.60.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 281ms, Maximum = 391ms, Average = 340ms
C:\>
```

Figure 10. Using ping to measure time distance between two points on the Internet.

variability is actually useful as it can be used as a way of quantifying the fluctuations in Internet conditions, much like measuring car speeds gives an indication of the level of road congestion.

Q. *What else can I do with ping?*

A. There are several ways that “pinging” Internet distances can be used to learn more about Net:Geography.

- First, and most obviously, a sequence of pings to the same place at different time periods can be used to build up a comprehensive longitudinal profile of latency. This might reveal interesting temporal patterns in the variation of latency as places on the Internet move nearer and further apart in a predictable fashion. Sudden changes in latency that do not fit the profile can reveal serious problems (e.g., a physical cut in a key fiber-optic cable).
- Another useful extension is to take pings from different places on the Internet to triangulate in on a particular target point. For example, one could take measurements of latency to *http://www.jasonnolan.net* not just from London, but from other geographically closer or and more distant points. The practicalities of doing this type of triangulation are made easier because there are a number of websites, which allow you to run pings from their location. (To find them use a search engine to look for “ping websites”.)
- By triangulating from different points it possible to get a sense of the relationship between latency and physical distance, assuming that the (approximate) geographic location of the origins and target are known. It is possible to get the physical distance (measured as the great circle distance) between the cities using a websites distance calculator (e.g.,

John A. Byers's site <http://www.wcrl.ars.usda.gov/cec/java/lat-long.htm>).

- Knowing the latency and physical distance also means you can approximate the speed of data transmission. Indeed, the use of ping has been taken further in a classroom physics experiment to calculate the speed of light. For technical details see Lepak and Crescimanno (2002).

5. ROUTES THROUGH THE INTERNET

Q. *What route does my data take through the Internet?*

A. You can answer this question using *traceroute*, a network engineer's tool that allows you to "lift the lid" on the Internet and get a "packets-eye" view of its working structure. It is undoubtedly one of the most useful tools available for Net:Geography fieldwork.

- Traceroute works in much the same way as ping but it provides much greater detail. It maps out the path that data packets take between two points on the Internet, showing all of the intermediate nodes traversed, along with an indication of the speed of travel for each segment of the journey.
- Traceroute was invented in 1988 by Van Jacobson at Lawrence Berkeley National Laboratory in the United States. The utility often comes as part of the operating system. The Windows version is called *tracert* and is used simply by typing, at the command prompt, *tracert [internet address, e.g., www.jasonnolan.net]*.
- Although, traceroute is primarily for network engineers to "debug" routing problems, it can also be used in a more tactical fashion by researchers to expose the political–economical structures of the Internet. It reveals the hidden complexity of data flows, showing how many nodes are involved (often more than twenty), the seamless crossing of oceans and national borders, and the sometimes convoluted transfers through networks owned and operated by competing companies.
- To illustrate how traceroute "maps" the Internet, it was used to chart the path from a PC in London to the <http://www.jasonnolan.net> website. Figure 11 shows the result.
- It is important to note that the view of data routing that is "seen" by traceroute is quite a generalized, "high-level" summary of the network in terms of topological connections. Below the traceroute view, there is a much more detailed level of routing in terms of the geography that lies between each node, based on the types of wires and their physical pathways in the ground. Sadly, this level of detail is not measurable using present Net:Geography fieldwork techniques.

```

Command Prompt
C:\>tracert www.jasonnolan.net
Tracing route to jasonnolan.net [64.246.60.38]
over a maximum of 30 hops:
  0  191 ms  180 ms  160 ms  webport-r12-hg9.ealing.ndip.bt.net [212.140.88.200]
  1  211 ms  180 ms  170 ms  192.168.1.38
  2  200 ms  160 ms  180 ms  interconnect5-10.ealing.fixed.bt.net [195.99.125.166]
  3  240 ms  531 ms  180 ms  core1-pos4-3.ealing.ukcore.bt.net [194.72.9.241]
  4  481 ms  1051 ms  301 ms  core1-pos10-0.redbus.ukcore.bt.net [194.74.65.254]
  5  1352 ms  *  *
  6  *  *  *  lndnuk1cx1.wcg.net [195.66.224.105]
  7  *  *  2774 ms  nyemny2wxc2-pos3-1.wcg.net [64.200.87.153]
  8  901 ms  631 ms  240 ms  hndvalwxc2-pos5-0.wcg.net [64.200.210.97]
  9  571 ms  251 ms  240 ms  hndvalwxc3-pos9-0.wcg.net [64.200.95.74]
 10  290 ms  271 ms  260 ms  drvlgalwxc2-pos4-0.wcg.net [64.200.232.125]
 11  301 ms  250 ms  261 ms  drvlgalwxc1-nc48.wcg.net [64.200.127.29]
 12  300 ms  290 ms  291 ms  dllstx1wxc3-pos6-0.wcg.net [64.200.240.21]
 13  330 ms  271 ms  280 ms  dllstx1wxc2-pos10-0-nc48.wcg.net [64.200.110.77]
 14  331 ms  270 ms  280 ms  hstntx1wcc2-pos4-0.wcg.net [64.200.240.74]
 15  331 ms  280 ms  271 ms  hstntx1wcc2-everyonesinternet-gige.wcg.net [65.77.93.54]
 16  *  721 ms  2043 ms  207.210.245.113
 17  320 ms  301 ms  270 ms  jessica.cpanelserver.co.uk [64.246.60.38]

Trace complete.
C:\>_

```

Figure 11. Traceroute from London to <http://www.jasonnolan.net>.

Q. This does not look much like a map, can you explain what it means?

A. The end result of a traceroute does look rather cryptic at first sight, but it is in fact a kind of one-dimensional map of how the data flows, with each node traversed listed on a separate line.

- The “map” gives a complete linear route listing showing how data packets traveled through the Internet starting in London and ending at Houston in the United States—the apparent location of the Web server which publishes <http://www.jasonnolan.net>. The three time measurements in milliseconds—such as 211, 180, and 170 ms—are round-trip times for that segment and give a useful indication of the speed of each link.
- Each node traversed is identified by its domain name and numeric IP address. Not all nodes have a domain name (e.g., 192.168.1.38). Also, notice that many nodes have strange, long domain names (e.g., *dllstx1wxc3-pos6-0.wcg.net*). These are routing computers at the core of the Internet and their domain names are not normally seen by users. With a little bit of “decoding” these router domain names can yield useful information, such as the type of node hardware, the bandwidth of the link, the name of ISP that owns a node and often a node’s approximate location (usually at the city level). Fortunately, for traceroute explorers, many of the large ISPs apply a consistent naming convention throughout their network infrastructures (as you can see from the domain names of nodes owned by *wcg.net* in Figure 11).
- The geographic location of the node is often represented in these types of domain names as an abbreviated city name. For example, *dllstx* at

the start of segments 12 and 13 (Figure 11) could sensibly be guessed to mean Dallas, Texas. Some ISPs use the familiar three letter airport identification codes (e.g., LHR for London Heathrow) as their city naming convention. (There are lists of these airport codes available on the Web, for example, at <http://www.orbitz.com/App/global/airportCodes.jsp>.)

Q. *How do I interpret the actual route to <http://www.jasonnolan.net> from the traceroute output?*

A. The first thing to note is that data traveling from London to <http://www.jasonnolan.net> had to pass through 16 intermediate network routers to reach the end of the destination (node 17). At least three different networks were traversed—British Telecom (BT), Williams Communication Group (WCG), and Everyones Internet.

- Reading the route line by line, it begins with the first node—how a user’s PC is connected to the Internet. From the domain name we can see that it belongs to *bt.net*. From local knowledge, it is known that “*ealing*” in the domain name is also an area in West London, so we can take this as an indicator of its likely geographic location.
- The next “hop” in the journey to node 2 is rather mysterious with no domain name to decode. We have to assume it is a node within BT’s network in London.
- Node 3’s domain name indicates it is another BT node in Ealing, London.
- Node 4 again says “*ealing*” and BT. The node also states “*ukcore*” which we might reasonably take to mean this node is within BT’s core network for the United Kingdom.
- Node 5 is also in BT’s “*ukcore*” network. Notice the increase in latency as measured by the RTT at this point in the journey.
- At “hop” 6 in the journey the data leave BT’s network and is handed off to another ISP called *wcg.net* (Williams Communication Group, now part of Wiltel corporation). The cryptic abbreviation at the start of the domain name (“*lndnuklicx1*”) can reasonably be decoded as London, U.K. The convention on this ISP’s network is to start the domain name with a four letter abbreviation of the city, followed by a two letter code for country/U.S. state. Note the big jump in RTT and the appearance of * for two of the times (this means timed-out, no response) at this point, probably due to traffic “congestion”.
- The next segment in the journey sees the data packets cross the Atlantic to New York, most likely on an undersea fiber-optic cable. The start of the domain name for node 7 is “*nycmny*” which can be decoded as New York City, New York. The RTT increases greatly at this point, again with two * timeouts.
- From New York the data travel on *wcg.net* network to “*hrndva*” at nodes 8 and 9 that are Herndon and Virginia (one of Washington D.C.’s

satellite towns which has a great deal of Internet infrastructure related companies).

- The next two steps in the journey on wcg.net's network are in "drvlga" which is somewhere in the state of Georgia. However, it is not immediately obvious which town "drvl" refers to. Perhaps it is a suburb of Atlanta, the main Internet hub point for the state.
- We are now approaching our goal, as the data move on into the state of Texas, going through Dallas ("dllstx") in nodes 12 and 13 and then to final destination, the city of Houston, Texas ("hstntx") at node 14.
- At node 15, the wcg.net network exchanges the data to a new company, EveryonesInternet (Everyones Internet, Inc.).
- Nodes 16 is most likely on EveryonesInternet network but does not have a domain name, so it is hard to know for sure.
- Node 17, somewhat confusingly called "jessica.cpanelserver.co.uk", is the domain name of the Web server that hosts <http://www.jasonnolan.net> website. It is quite unclear why this server in Houston has a *co.uk* domain name!
- It is important to realize that Internet routing is dynamic, it can change minute by minute. The "map" that is produced by traceroute is a live scan and always represents a one-off snapshot of Net:Geography at the point in time it was charted. Running the same trace at a future time is quite likely to give a different map.

Q. *Can I run traceroutes from different places?*

A. Yes, just like ping you can "triangulate" the Internet using Web-based traceroutes.

- These make it possible run traces from many different starting points, including on different networks and in completely different continents. Web traceroute gateways are very useful for active exploration of the Internet's topology from across the globe and illustrate the degree to which routes vary.
- There are several hundred freely available Web traceroute gateways in many places. Thomas Kernen maintains a good list of them at <http://www.traceroute.org>.
- As an example of traceroute triangulation we ran a trace from Australia to <http://www.jasonnolan.net> using a gateway provided publicly by Telstra, the main Australian telecoms carrier. Figure 12 shows the output "map" from the trace. (Note that the formatting of this output is slightly different to that produced by Windows tracert.)
- Again, with a little bit of decoding work, reading line by line, it is possible to follow the data packets on this new journey. The traceroute utility is installed on a *telstra.net* server located in Canberra, Australia indicated by the domain name for node 1. The next two nodes in the trace were also within Canberra, according to their domain names.

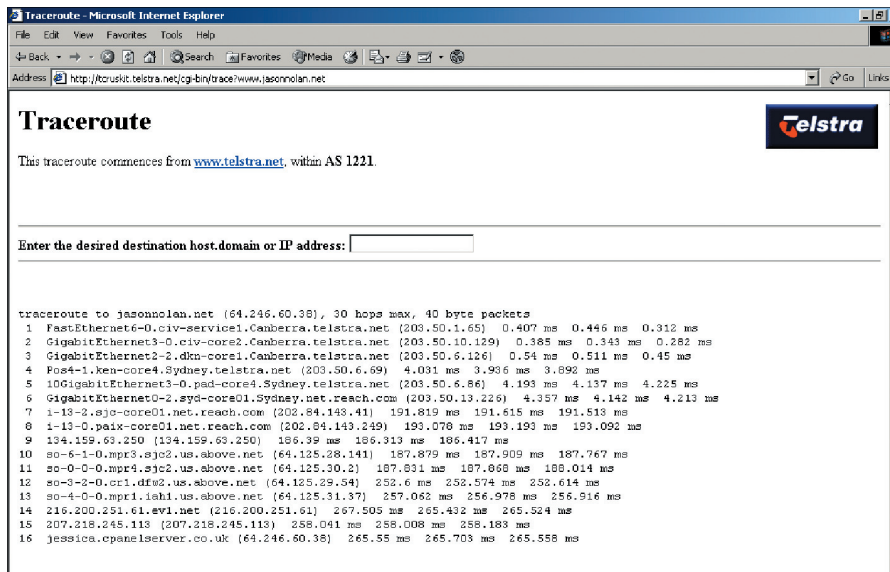


Figure 12. An example of a Web-based traceroute from Canberra, Australia to <http://www.jasonnolan.net> (Available at <http://www.telstra.net/cgi-bin/trace>).

- At node 4 the data moved a couple of hundred miles on the *telstra.net* network from Canberra to Sydney. The data are then passed through three nodes in Sydney before leaving the Telstra network for the *reach.com* network at node 6.
- The big trans-Pacific hop in the journey occurred at node 7, as the data went to “*sjc*”, the airport code for San Jose, California. Note, the marked jump in the RTTs at this point in the journey, caused in large part by the 7500-mile distance across the Pacific Ocean.
- Node 8 on the *reach.com* network is located at “*paix*”, the name of a major Internet exchange point located in Palo Alto, California. Node 9 is cryptic. At node 10, the data left PAIX for a new network that of *above.net*.
- Nodes 10 and 11 on *above.net*’s network were located in San Jose, California as indicated by the “*sjc*” codes in their domain names.
- The data moved on from California into Texas, going to Dallas-Fort Worth (“*dfw*”) at node 12. It moved onto Houston, Texas (“*iah*”) at node 13.
- The final stretch into <http://www.jasonnolan.net> took place at nodes 14 and 15, which are likely to still be in the Houston area.

Q. Can I geographically map traceroute output?

A. Yes, an obvious refinement of the regular traceroute list output is to try to plot the route visually on a geographic map. There have been a

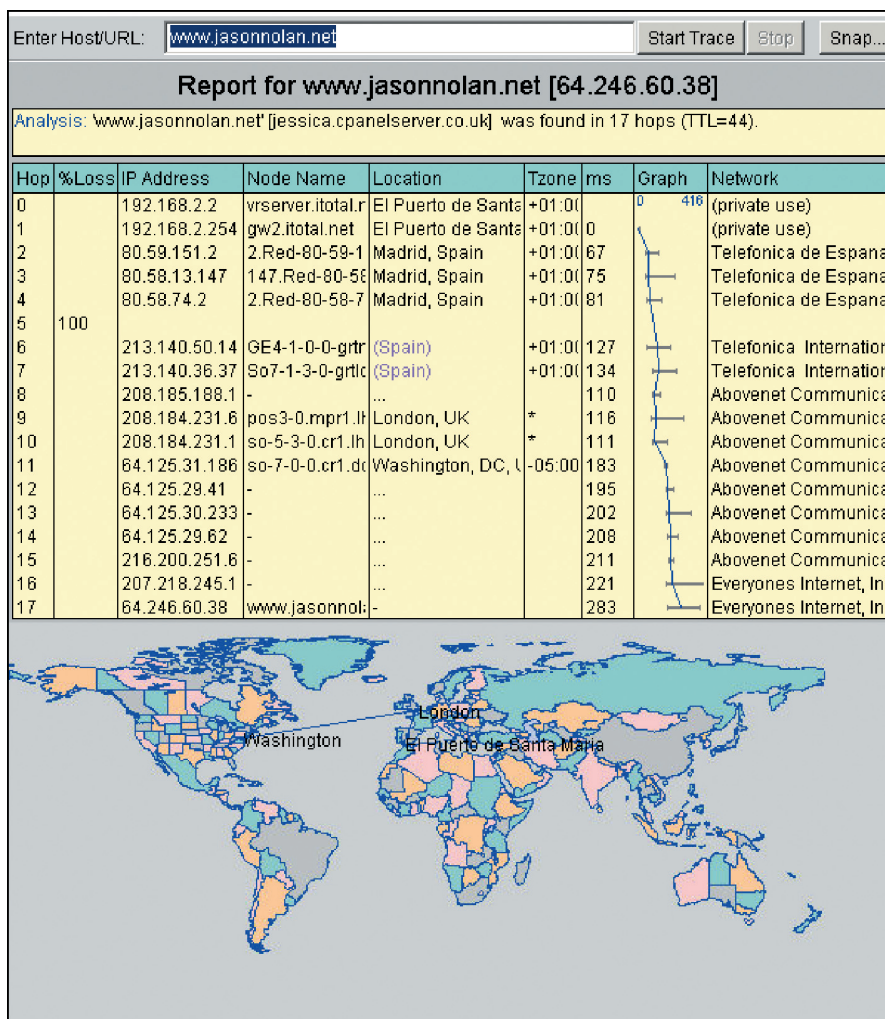


Figure 13. An example of a geographic traceroute produced using VisualRoute.

number of attempts at a geographical traceroute, with varying degrees of success.

- Figure 13 is a screenshot of the best geographic traceroute program currently available, called VisualRoute (<http://www.visualroute.com>), tracing the data route from a server in Spain to <http://www.jasonnolan.net>. The top half of the display is table presentation of the trace results. The approximate locations (where known) of the routers are plotted on a rather crude map below.
- The particular advantage of this application is the ease of geographic interpretation of routing. For example, it can provide direct visual

evidence of the Internet's business "logic" of data routing following the cheapest paths rather than the geographical shortest. Much international Internet traffic is still routed through the United States as the cheapest means of transit between regions. This can result in sometimes quite anomalous looking, circuitous routes being chosen.

- However, automated geographic traceroute is far from perfect. It is very hard for software to reliably "decode" the router domain names, as this often requires local knowledge, human intuition, and a bit of guesswork. The large number of gaps in the "Location" column of the traceroute results table in Figure 13 clearly show the limitations.

Q. *What else can I tell from traceroute results?*

A. There are practical things you can use traceroute data for. It can also be used for more political "debugging" of the Internet's structure.

- Traceroute can be really useful for deducing the approximate location of Internet hosts (such as websites) in terms of "hardware geography". The output can tell you the location and identity/owner of the "upstream" network provider even if the final destination of the server is unclear. If the data travel into a certain city and does not leave it again, it is probable that the target is located there. For example, deducing that <http://www.jasonnolan.net> is published from a Web server in Houston, Texas. Also, the "upstream" network providers may keep logs for identifying a host that is of interest (this is of particular concern for law enforcement agencies in tracing the source of illegal activities).
- Traceroute has also been used in a physics classroom experiment to measure the size of the earth. See Kicovic et al. (2002).
- Running multiple traceroutes to lots of different points across the Internet has also been used to gather data to chart the topology of the core of Internet. The results of which have been impressively visualized as huge abstract graphs, providing some of the most evocative representations of Net:Geography. See for example Lumeta's Internet Mapping Project (<http://lumeta.com/mapping.html>) and Branigan et al. (2001).
- Traceroute can also reveal something of the hidden political economy of Internet. The patterns of traffic routing shows transit agreement and mutual peering relationship between competing companies. Details on these deals are often deemed commercially confidential but are revealed by necessity in how and where the actual networks interconnect to share data. The routing of traffic reveals the structuring of business relationships in terms of who connects to whom and the hierarchy of these connections (from periphery to center to periphery again). It can also show which telecommunications carriers dominate the transfer of traffic between certain countries and between continents. These companies are likely to be influential in the structuring of global communications

and tracerouting could provide an alternative way to quantify the extent of their power.

- Traceroute can show potential vulnerabilities in the structure of the Internet. Are there particular choke points in the routing of data flows? Is there only single route into a region or between two cities?
- Lastly, the output from traceroute provides a useful way to assess the number of international borders crossed and determines which different territories (i.e., separate legal jurisdictions) the data transit. The more “points of contact” in the flow from origin to target, the more potential there is that Internet traffic could be intercepted and subjected to local regimes of monitoring, filtering, censorship, and data retention. For example, does an e-mail message transit through a third-party nation that has hostile intentions. Particularly in regions of conflict, being able to identify territories that are transited might be vitally important in terms of the reliability of communication. For example, does an e-mail to someone in Palestine transit through Israel?

CONCLUSION

Q. *So what is the future of Net:Geography fieldwork?*

A. As the Internet grows in size, expands in scope, and becomes increasingly embedded as a banal and invisible background to everyday living, it becomes more important to understand its politics. We would argue that understanding the geographies of the Internet, through Net:Geography fieldwork using the techniques and tools described here, provides one of the most valuable avenues into network politics, allowing you to gather information firsthand and critically question network operations directly.

- Net:Geography fieldwork is likely to become easier as new and more powerful software tools for scanning the structure of Internet become available. This will be a benevolent outcome of the experience in the design of the current plague of Internet worms and viruses and ways to counter them. Also, as search engine tools develop they will increasingly provide new ways to do Net:Geography fieldwork in terms of mapping the information structures on the Internet. Of course, researchers will continue to have to tread carefully the ethical boundaries between critical fieldwork and potentially criminal hacking.
- Yet, at the same time, Net:Geography fieldwork is also going to get harder and riskier to do. Individual networks on the Internet are increasingly being designed and operated in a much more closed fashion. For example, the university networks of the authors have recently begun blocking ping and traceroutes as a security precaution against malicious scanning. Other areas of the Internet are also using the cover of greater security as a way to try to develop more proprietary and profitable

business operations. While many Internet users, for example on peer-to-peer networks, are likely to be using software tools in future that encrypt and cleverly attempt to mask their activities and their locations to preserve confidentiality of communication in the face of evermore draconian monitoring by corporations and governments. This will also have a side effect of frustrating Net:Geography fieldwork.

- Despite these changes, Net:Geography provides a very useful set of virtual learning tools for interrogating the media that supports virtual learning itself. They can reveal important details about the geography of infrastructure, the linking of information, differential access to resources, and so on. They therefore constitute a useful resource to those interested in virtual learning.

REFERENCES

- Branigan, S. Burch, H. Cheswick, B., & Wojcik, F. (2001). What can you do with traceroute? *Internet Computing* 5(5), 96. Available at: <http://computer.org/internet/v5n5/index.htm>.
- Clayton, R. (2001). The Limits of Traceability. Available at: http://www.cl.cam.ac.uk/users/rnc1/The_Limits_of_Traceability.pdf.
- Kicovic, S., Webb, L., & Crescimanno, M. (2002). Measuring the Earth with Traceroute. Available at: <http://arxiv.org/abs/physics/0208087>.
- Lakhina, A. Byers, J. W., Crovella, M., & Matta, I. (2002). On the geographic location of Internet resources. *Technical Report 2002-15*, Computer Science Department, Boston University. Available at: <http://www.cs.bu.edu/techreports/pdf/2002-015-internet-geography.pdf>.
- Lepak, J. & Crescimanno, M. (2002). Speed of light measurement using ping. *Report No. YSU-CPIP/102-02*. Available at: <http://arxiv.org/abs/physics/0201053>.
- Padmanabhan, V. N. & Subramaniann, L. (2001). Investigation of Geographic Mapping Techniques for Internet Hosts. *SIGCOMM'01*, August 27–31, 2001, San Diego. Available at: <http://www.research.microsoft.com/~padmanab/papers/sigcomm2001.pdf>.
- Reporters without Borders. (2003). The Internet Under Surveillance: Obstacles to the Free Flow of Information Online. Available at: <http://www.rsf.org>.
- Searls, D. & Weinberger, D. (2003). World of Ends: What the Internet is and How to Stop Mistaking it for Something Else. Available at: <http://www.worldofends.com>.