The Workshop on Active Internet Measurements (AIMS) Report

kc claffy
CAIDA
kc@caida.org

Marina Fomenkov
CAIDA
marina@caida.org

Ethan Katz-Bassett
University of Washington
ethan@cs.washington.edu

Robert Beverly
MIT CSAIL/BBN
rbeverly@csail.mit.edu

Beverly A. Cox
Laboratory for
Telecommunications Sciences
beverly.a.cox@ugov.gov

Matthew Luckie
University of Waikato
mjl@luckie.org.nz

This article is an editorial note submitted to CCR. It has NOT been peer reviewed. The author takes full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

Measuring the global Internet is a perpetually challenging task for technical, economic and policy reasons, which leaves scientists as well as policymakers navigating critical questions in their field with little if any empirical grounding. On February 12-13, 2009, CAIDA hosted the Workshop on Active Internet Measurements (AIMS) as part of our series of Internet Statistics and Metrics Analysis (ISMA) workshops which provide a venue for researchers, operators, and policymakers to exchange ideas and perspectives. The two-day workshop included presentations, discussion after each presentation, and breakout sessions focused on how to increase potential and mitigate limitations of active measurements in the wide area Internet. We identified relevant stakeholders who may support and/or oppose measurement, and explored how collaborative solutions might maximize the benefit of research at minimal cost. This report describes the findings of the workshop, outlines open research problems identified by participants, and concludes with recommendations that can benefit both Internet science and communications policy. Slides from workshop presentations are available at http://www.caida.org/workshops/isma/0902/.

Categories and Subject Descriptors

C.2.3 [**Network operations**]: Network monitoring; C.2.5 [**Local and Wide-Area Networks**]: Internet; C.2.6 [**Internetworking**]: Standards; C.4.2 [**Performance of Systems**]: Measurement techniques—Active

General Terms

Measurement, Management, Human Factors, Legal Aspects, Standardization, Performance, Verification

Keywords

active measurement, measurement techniques, management techniques, codes of ethics, codes of good practice, validation

1. MOTIVATION

Collecting representative Internet measurement data has remained a challenging and often elusive goal for the networking community. Obstacles include the Internet's scale and scope, technical challenges in capturing, filtering and sampling high data rates, difficulty in obtaining measurements across a decentralized network, cost, and political hurdles [9]. Yet, as with other complex system sciences (climate, biology, sociology), data is, while not sufficient, absolutely necessary to progress.

The Internet research community has developed dozens of novel techniques, practices, and infrastructures in pursuit of understanding as well as empirical grounding for various models of Internet structure and behavior. Most measurement methods are typically classified as either "passive" or "active." Passive measurement relies on a observation point within the network capturing live data from a portion of the network. Internet packet header traces from a core high-speed link interconnecting many networks and representing even more individual user communication flows, are a canonical example of passive data from the Internet. In contrast (but often complementary as a measurement technique), active measurements generally refer to techniques that inject targeted traffic, i.e. specially crafted probes, across the network in order to infer characteristics of network workload, topology, performance, policy (engineering or business), vulnerabilities, etc.

The Active Internet Measurements (AIMS) workshop convened on February 12-13, 2009, focused on recent advances, challenges, and goals in active measurement. The workshop was motivated by CAIDA's recent DHS[1] and NSF[2] Archipelago (Ark) [17] – a new active measurement platform providing a coordination and communication facility for macroscopic distributed Internet measurements, which relied on ideas discussed at a previous community workshop [7] where participants were adamant about the need for better Internet topology data as well as more functional access to existing data, e.g., standard derived data sets.

Ark is composed of 35 nodes (as of June 2009) capable of flexible probing of IPv4 address space. Six of those nodes are IPv6-capable as well. We designed Ark to shield researchers from the complexities of network communication and faults, aiming to lower the barrier to deploying sophisticated and fine-grained distributed measurement experiments. Ark provided data to researchers who want to analyze the Internet topology to investigate open questions such as graph (in)completeness [25], Ark also has supported other researchers in need of controlled and coordinated vantage points to study the efficiency of various probing methods [19] and to assess macroscopic network hygiene [3]. CAIDA wants to make sure Ark benefits Internet researchers worldwide, and a forum like AIMS helps us and others to solicit feedback on progress with community Internet measurement infrastructure development. Another goal of the workshop was to discuss development of a set of measurement principles to guide efficient and ethical use of resources in the scientific community [5, 24].

The workshop achieved its basic goals: researchers, operators, and policy makers exchanged ideas, presented new techniques

[1] U.S. DHS Science and Technology Directorate, Cybersecurity Program, Contract #N66001-08-C-2029.

[2] NSF Computer and Networked Systems CRI-0551542.

and findings, and outlined recommendations for the Internet measurement community moving forward. Topics presented included tools and infrastructure for measuring performance, bandwidth estimation, traffic discrimination, botnet identification, spoofability detection, prevalence of source address validation filtering, and traffic discrimination. This paper summarizes these key findings and recommendations from the workshop.

2. KEY FINDINGS

The longevity of measurement infrastructure is crucial, yet often overlooked and underfunded.
Research projects come and go in resonant frequency with funding opportunities. While many measurement projects successfully answer important research questions, the project's measurement infrastructure typically dies after funding is exhausted. Longitudinal data collection and analysis is a crucial missing piece of network science; U.S. policymakers are now acutely exposed to this gap in attempting to establish a national broadband plan. Policymaking agencies (FCC, NTIA), with less experience than NSF and DHS in funding computational science instrumentation, are now starting to recognize the need for instrumentation for long-term Internet measurement.

Measurement platforms: several active measurement infrastructures are available for use by researchers .
Several Internet measurement research projects perform active measurement of the global Internet, including gathering long-term trends, despite challenges in keeping them funded. Each project serves a different goal, enables a different measurement, or provides a different approach. This workshop provided a rare opportunity to discuss how various projects could leverage each other's infrastructures. Historically, the field has had a strong focus on measurements of macroscopic topology and on improvements to methodologies for accurately capturing and validating Internet topology. More recently researchers have also turned their efforts toward performance measurements, in the wake of network neutrality conversations. Table 1 lists in alphabetical order some of the most well known and frequently used systems that make their measurement data publicly available. Some of them also are open for researchers to propose and conduct their own experiments.

The projects listed in Table 1, each with different costs, advantages, and limitations, illustrate a range of models for supporting network measurement. Many projects integrate components (tools or data) into the platform for use by the larger Internet research community [16]. Common challenges are: (i) how to coordinate measurement requests from a large community of researchers, and (ii) how to ensure integrity of the data gathered by an unknown party. Workshop participants realize that a long-term strategy for active Internet measurement infrastructures is a priority, but in most countries there is no clear source of funding for it, so it was not a primary focus of discussion.

Policies: workshop participants agreed that consistent, transparent, and straightforward policies providing guidance for conducting experiments and sharing the resulting data are long overdue.
The first attempt to develop a code of conduct for any Internet research happened in 1991, when the explosive growth of Internet usage beyond the R&E community was just beginning. Vint Cerf published RFC1262, *Guidelines for Internet Measurement Activities* [8], a brief (less than 120 lines) document emphasizing that Internet measurement and data collection are vital to the future of the Internet, and offered a list of broad conditions for proper professional and ethical active measurement, e.g., Condition #1 is: "The data collected will not violate privacy, security, or acceptable use concerns".

There was strong consensus at the workshop that updating these documents would benefit the research and funding community. Now, two decades later, the Internet permeates all aspects of our lives: personal, professional, and political. An experiment that disrupts the smooth functioning of the Internet will have widespread and possibly devastating consequences. Service providers are concerned about customer reactions, wasted efforts of personnel responding to attack-like behavior, and possibility of financial loss; they tend to avoid unnecessary risk, and often explicitly block the ability for others to measure their networks. Such explicit efforts on the part of providers to block measurement or otherwise conceal information about their networks demonstrates the misalignment of incentives. But some providers are increasingly willing to collaborate and share data on their infrastructures with researchers to achieve security or other operational goals; in Japan, Internet providers even allow researchers access to aggregated traffic statistics.

Active measurement data generates fewer privacy concerns than exist with passive (traffic) data, but knowledge of Internet topology can facilitate attacks and other malicious behavior. Balancing individual privacy protection against other goals, such as national security, critical infrastructure protection, and science, will always remain a challenge in a networked world. DHS is currently the only U.S. government agency proactively seeking to enable privacy-sensitive data sharing for Internet security research [5], but is still confined by economic (resource) and legal issues, which will likely take a crisis (and/or another agency) to resolve. Nevertheless, privacy-respecting data sharing frameworks are prerequisite to effectively studying most fundamental Internet research questions [2].

3. RESEARCH ENABLED (OPEN PROBLEMS)

Workshop participants identified research topics that motivate and inspire active data collection and analysis efforts:

1. *Evaluate end user perceived performance (network neutrality).* Researchers want to build and improve tools to validate the advertised bandwidth capability of one's broadband connection, and in particular to detect any discriminative filtering.

2. *Construct AS/Points-of-Presence (PoP) level maps.* In AS-PoP maps each node represents a group of routers, such as a small stub AS or a PoP of a large or medium size AS. Such maps offer a relatively accurate representation of the Internet topology, bridging the gap between representations at the AS and the IP levels. Operators, application designers, and researchers could benefit from such maps annotated with link characteristics, e.g., delay, bandwidth, business relationships, geography. Realistic AS-PoP maps also provide empirical grounding for modeling and simulating routing protocols, and well as support DHS's Internet infrastructure protection mission.

3. *Explain the accumulation of IP links over time.* Several researchers have noted linear growth of the number of observed IP links over time. Currently there is no definitive explanation for this suspiciously linear growth; some hypothesize it may be an artifact of data collection methods, specifically an inability to prune links that no longer exist [27].

4. *Testing reachability of newly allocated address space.* Many operators maintain filters that prevent traffic from IP addresses that are unassigned or otherwise deemed inappropriate to appear in packets. It is challenging to determine whether IP addresses are reachable from given address space without actually attempting to send traffic from that address space. Broadly deployed measurement infrastructures allow for testing reachability, which will become increasingly important as the IPv4 address supply reaches exhaustion.

5. *Measuring the provision of security mechanisms.* Macroscopic surveys can assess network hygiene practices, such as prevalence of deployed filtering of spoofed packets [3] or testing DNS caching resolvers for vulnerability to cache poisoning [30].

6. *IPv6 deployment penetration.* Whether IPv6 happens will be determined by, and will in turn determine, other important aspects of the Internet's evolution. An IPv6-capable

Platform	Organization	# of nodes	data interval	Data type	Motivation	Funded by	Ref
Ark	CAIDA	32	daily	IP/AS topology	create annotated Internet maps	DHS, NSF	[17]
Dimes	Tel-Aviv University	19,000 (home users)	monthly files	IP/AS topology	capture peripheral topology	EU/HU	[29]
Etomic	EVERGROW Consortium	18		IP-level paths	synchronized active measurements	EU	[22]
Grenouille	Grenouille Association	>100,000 (home users)			Internet service quality monitoring	volunteer	[12]
Gulliver	WIDE	28	varying	DNS probes	low cost/maintenance active measurement platform	NICT / WIDE	[28]
M-lab	Google	6		performance varying	measure network neutrality	researchers	[11]
PlanetLab	PlanetLab Consortium	423	varying	varying	global testbed for dist. systems experiments	NSF / members	[1]

Table 1: Summary of available measurement infrastructures.

active measurement infrastructure would allow for a neutral source of data on IPv6 connectivity, reachability, performance, and growth.

7. *System dynamics at various time scales.* The Internet has organic aspects to its growth and evolution, on many different time scales from seconds (load balancing) to years (ISP topologies). Capturing these dynamical phenomena on both short and long time scales is prerequisite to developing more realistic explanatory models of Internet structure, behavior, and evolution [26].

8. *Geolocation of IP resources.* While commercial IP geolocation tools exist [6], they tend to use proprietary methodologies, offer poor granularity, and often disagree with each other on locations. Some groups (W3C, IETF GeoPriv WG) are trying to standardize on interfaces to support location-aware Internet services, but progress is slow. Several participants suggested the community prioritize an objective assessment and comparison of various available geolocation tools. In the meantime, researchers often use MaxMind [21] or try to develop their own heuristics [13].

9. *Future routing.* Routing scalability is one of the most serious threats to future Internet stability and growth. Recent discoveries [4] reveal that routing processes in complex network are inextricably coupled to their structural and topological properties. More accurate knowledge of Internet topology will inform discussions of future Internet architectures, as well as how to better manage this one.

10. *Network science.* The Internet is just one example of a complex network, others are social, biological, transport [10]. Finding fundamental laws governing behavior and evolution of complex networks will profoundly affect multiple scientific disciplines [4].

3.1 Validation

Validation of inferences and models against real data is a necessary prerequisite to rigorous investigation of Internet science, including all of the research areas listed above. Participants of the Workshop in Internet Topology (WIT) in 2006 drew attention to this problem stating in the workshop report [7] that “Predictive models of the Internet topology and evolution cannot be developed without validation against real data.” They also concluded that “A lack of comprehensive and high-quality topological and traffic data represents a serious obstacle to successful Internet topology modeling, and especially model validation.” Unfortunately, as with many other types of Internet measurement, the problems are rooted in issues of economics, ownership, and trust [15] rather than anything technical. Although providers have started to express interest in protected data sharing, the most practical method of identifying strengths and weaknesses of each inference method remains comparing them to eachother (e.g., [20]), rather than ground truth. Another common validation technique is to use small and not necessarily representative sets of ground truth data, such as topologies of educational networks, or rely upon public information, such as well-known outages reported on mailing lists. Researchers informally accumulate lists of researcher-friendly contacts at network providers who offer helpful data for validation, but there is no standard community model for this exchange.

Since the Internet infrastructure is operated by a conglomerate of private enterprises, progress in validation requires a concerted (and often time-consuming) cooperative efforts between researchers and ISPs, but operators lack incentive and capital to devote to this collaboration. Worse, unrelenting commercial, security and legal pressures dictate proprietary ISP policies and render it nearly impossible to afford researchers even a glimpse into the underpinnings of Internet operations. The situation may change someday, but not likely soon.

3.2 Novel measurement techniques

Researchers are constantly looking to widen the arsenal of available active measurement techniques. Among the challenges discussed at the workshop were:

1. *Coordination of measurements among vantage points* to allow more flexible deployment of different monitor teams performing multiple experiments.

2. *Tools expanding the existing range of probing types* to include various Level 2 protocols, MPLS, IP tunneling, and various cryptographic protocols.

3. *Hybrid tools* combining both active (traceroute) and passive (BGP) methods of data collection in real time.

4. *Tools for IPv6 address space measurements* of IPv6 topology, performance, and penetration. Ark monitoring infrastructure began regular probing of the IPv6 space (although on a limited basis) in December 2008.
5. *IPv4 reachability/filtered measurements* that will grow in importance in the near future as IPv4 address space is approaching its exhaustion.
6. *Tools to measure characteristics of wireless clouds* that will become more sensitive, as wireless communications expands to ubiquity.
7. *Correlation of topology and traffic*, which has made little progress for data availability reasons.
8. *Scalable topology measurement tools*, e.g., that can efficiently probe every /24 network or, at least, every routable prefix in the global BGP tables.
9. *Tools enabling general public participation* in Internet measurements.

Examples of this latter approach presented at the workshop are: DIMES [29] where users probe the Internet from their home computers; MIT's spoofer, where users can detect whether spoofing is allowed from their computer's network [3]; Grenouille [12], which allows users to monitor their own performance and sources of service degradation they experience; and Google's M-lab [11], which makes tools and services available for end users to test their own connectivity and performance. The most famous such Internet measurement tool on PlanetLab is Hubble [14], launched last year, which allows users to monitor wide-area reachability problems taking advantage of PlanetLab's globally distributed topology. Such "user-centric" approaches have achieved coverage not conceivable with a singly administered cloud approach.

3.3 Guidance

Legal constraints relating to Internet measurement – most of which predate the Internet – are intended to protect the privacy of individual communications. Yet conservative interpretations of communication laws, established long before the Internet was created, leave researchers and policymakers trying to analyze the global Internet ecosystem essentially in the dark.

How can we find a balance between privacy and science? Other fields may offer guidance. Medicine has been dealing with protection of human subjects for over a century. As a response to several disturbing experiments in the field that raised public scrutiny, in 1979 the U.S. government issued the Belmont report [24] – "Ethical Principles and Guidelines for Research Involving Human Subjects" – to establish risk-benefit criteria in the assessment of research experiments. The Belmont report also clarified the concept of *informed consent* in various research settings. (DHS hosted a workshop in May 2009 for Internet researchers to discuss creating their own "Belmont report" defining acceptable boundaries of Internet experiments and subsequent data use and sharing [18].)

DHS (through the PREDICT project) has also advised establishing a working relationship with the office of Human Research Protections Program (HRPP) (or analogue) that exist on every campus to supervise medical, biomedical, and sociological research programs. These offices assist researchers in complying with federal, state and university policies regarding experimentation involving human subjects, and oversee the review and conduct of research conducted by federally registered Institutional Review Boards (IRBs). [3]

4. RECOMMENDATIONS

The research community needs to introduce and agree upon standards and best practices to promote a diverse and heterogeneous field of Internet active measurements. Workshop participants emphasized that standardization is extremely important as it will ensure the reproducibility and enhance the validity of measurement results. The context is a growing realization that infrastructure, platform, tools, measurement, and measurement consumers can often be separated to take advantage of expertise and reuse opportunities. Examples include:
(i) develop standard APIs for measurement systems, standardize tool output, enable tool sharing on different platforms;
(ii) publicize the best available data, document them as ground truth, provide comprehensive statistical characterization, make these data easily downloadable;
(iii) design flexible, easily extensible measurement infrastructure platforms capable of running various tools and types of measurements at Internet scale;
(iv) provision for continuity of measurements, dissemination of data, with long-term archiving of data to study historical trends;
(v) maintain no-probe lists based on requests

The lack of consistent guidelines for Internet measurement limits the recognized legitimacy of Internet measurement systems. Participants recognize that there are currently no guidelines for navigating EOT (economics, ownership, and trust) issues associated with Internet measurements. Next steps to address this problem include:
(i) replace obsolete RFC1262 with a more current document;
(ii) create a "Belmont report" for Internet research;
(iii) facilitate interaction between Internet researchers in Institutional Review Boards (IRB) that overview and regulate human research activities at individual institutions;
(iv) identify important research questions/problems in the field of Internet research where macroscopic active measurement can have a positive impact.

The research community must increase transparency of Internet measurements and better communicate utility of results to broader communities affected by measurements (legal, political, operators, users). Transparency plays an important role in alleviating concerns. Possible approaches include:
(i) create a central easily accessible database of planned or ongoing Internet experiments
(ii) release source code for tools used for publications
(iii) consider other means of communication (i.e., blogs, mailing lists, automated announcements) to keep other communities informed of Internet measurement research experiments;
(iv) increase visibility and usability of data (including formatting standards [23]), relevance of data to users, and exposure of implications of studies based on data
(v) inform debate about clean-slate Internet architecture;
(vi) discuss with academics, operators, and funding agencies how many measurement infrastructures are needed, for what purposes, and if there are more effective ways of funding them;
(vii) enable interaction and technology transfer between three main players in the field of Internet research: academic laboratories, commercial enterprises, and government institutions.

ACKNOWLEDGMENTS. The workshop was supported by the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate via contract N66001-08-C-2029. We thank all participants for their insights.

5. REFERENCES

[1] Planetlab. http://www.planet-lab.org/consortium.
[2] Mark Allman and Vern Paxson. Issues and etiquette concerning use of shared measurement data. In *IMC*, 2007.
[3] Rob Beverly. Spoofer project. http://spoofer.csail.mit.edu/index.php.
[4] Marian Bogun a, Dmitri Krioukov, and K. C. Claffy. Navigability of complex networks. *Nature Physics*, 5:74–80, 2009.
[5] CAIDA. The DHS PREDICT project. http://www.caida.org/projects/predict/.

[3] In October 2008 CAIDA's first application to the UCSD HRPP office requesting review of our research protocol by the campus IRB was approved.

[6] CAIDA. Netgeo ref. http://www.caida.org/utilities/netgeo/.

[7] CAIDA. Workshop on Internet Topology, 2006. http://www.caida.org/workshops/isma/0605/.

[8] Vint Cerf. *Guidelines for Internet Measurement Activities*. IETF, RFC 1262, Oct 1991.

[9] National Research Council Committee on Research Horizons in Networking. *Looking Over the Fence at Networks: A Neighbor's View of Networking Research*. National Academies Press, 2001.

[10] S. N. Dorogovtsev and J. F. F. Mendes. *Evolution of Networks: From Biological Nets to the Internet and WWW*. Oxford University Press, Oxford, 2003.

[11] Google. Measurement lab (m-lab). http://www.measurementlab.net/about.

[12] Grenouille. Collaborative monitoring. http://wiki.grenouille.com/index.php/CMON\#Technical_and_scientific_description_of_the_activities.

[13] Ethan Katz-Bassett, John P. John, Arvind Krishnamurthy, David Wetherall, Tom Anderson, and Yatin Chawathe. Towards IP geolocation using delay and topology measurements. In *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 71–84, 2006.

[14] Ethan Katz-Bassett, Harsha V. Madhyastha, John P. John, Arvind Krishnamurthy, and Thomas Anderson. Studying black holes in the Internet with Hubble. 2008. http://www.cs.washington.edu/homes/ethan/papers/hubble-nsdi08.pdf.

[15] kc claffy. Ten things lawyers should know about the internet. http://www.caida.org/publications/papers/2008/lawyers_top_ten/.

[16] kc claffy, Mark Crovella, Timur Friedman, Colleen Shannon, and Neil Spring. Community-Oriented Network Measurement Infrastructure (CONMI) Workshop Report. *ACM SIGCOMM Computer Communication Review*, 36(2):41–48, 2006.

[17] kc claffy, Young Hyun, Ken Keys, Marina Fomenkov, and Dmitri Krioukov. Internet mapping: from art to science. In *CATCH*, 2009.

[18] Erin Kenneally and kc claffy. What's belmont got to do with it?, May 2009. http://blog.caida.org/best_available_data/2009/06/12/whats-belmont-got-to-do-with-it/.

[19] Matthew Luckie, Young Hyun, and Bradley Huffaker. Traceroute probe method and forward IP path inference. In *Internet Measurement Conference*, October 2008. http://www.caida.org/publications/papers/2008/traceroute_probe_method/.

[20] Priya Mahadevan, Dmitri Krioukov, Marina Fomenkov, Bradley Huffaker, Xenofontas Dimitropoulos, kc claffy, and Amin Vahdat. The Internet AS-level topology: Three data sources and one definitive metric. *Computer Communication Review*, 36(1), 2006.

[21] MaxMind. Maxmind geolocation technology. http://www.maxmind.com/.

[22] D. Morato, E. Magana, M. Izal, J. Aracil, F. Naranjo, F. Astiz, U. Alonso, I. Csabai, P. Haga, G. Simon, J. Steger, and G. Vattay. The European traffic observatory measurement infraestructure (ETOMIC). In *TRIDENTCOM*, 2005. http://www.etomic.org/.

[23] Saverio Niccolini, Sandra Tartarelli, Juergen Quittek, Thomas Dietz, and Martin Swany. Information model and XML data model for traceroute measurements. http://www.ietf.org/rfc/rfc5388.txt.

[24] National Institutes of Health. Ethical principles and guidelines for the protection of human subjects of research (the belmont report), Apr 1979. http://ohsr.od.nih.gov/guidelines/belmont.html.

[25] Ricardo Oliveira, Dan Pei, Walter Willinger, Beichuan Zhang, and Lixia Zhang. Quantifying the completeness of the observed AS-level structure. http://www.cs.ucla.edu/~rveloso/papers/completeness_tr.pdf.

[26] Romualdo Pastor-Satorras, Alexei Vazquez, and Alessandro Vespignani. Dynamical and correlation properties of the internet. *Physical Review Letters*, 87:258701, 2001.

[27] Pedram Pedarsani, Daniel R. Figueiredo, and Matthias Grossglauser. Densification arising from sampling fixed graphs. In *Proceedings of ACM SigMetrics*, June 2008. http://infoscience.epfl.ch/record/126463/files/1569084170-pedarsani.pdf.

[28] Yuji Sekiya, Kenjiro Cho, , and Yohei Kuga. Gulliver project. http://gulliver.wide.ad.jp/.

[29] Y. Shavitt and E. Shir. DIMES: Let the Internet measure itself. *Computer Communication Review*, 35(5), 2005.

[30] Duane Wessels. DNS survey: Open resolvers, 2009. http://dns.measurement-factory.com/surveys/openresolvers.html.