Investigating Identifier Systems Abuse or Misuse: Training Metrics

ICANN Office of the CTO
Security, Stability and Resiliency Team | 3 February 2017

Introduction

As part of its role and remit, the ICANN Office of the CTO (OCTO) Security, Stability and Resiliency (SSR) team provides capability training to anti-abuse communities. Recipients of this training include computer emergency response teams (CERTs), national law enforcement and justice departments, nongovernmental agencies involved with cybersecurity, national cybercrime or cybersecurity agencies, and international agencies – including Europol and Interpol. In June 2016, the team agreed on a standard form for soliciting feedback from training recipients. This form asks 10 questions and allows the trainee to provide written comments.

This report covers the period from September to December 2016 following eight training sessions conducted by Dave Piscitello, VP of Security and ICT Coordinator, or Richard Lamb, Senior Program Manager of DNS Security Extensions (DNSSEC). Training recipients were from the U.S. Department of Justice, Interpol (Underground Economy 2016), Austrian Cyber Competency Center, Dubai, Doha, Beirut (two) and the Republic of Georgia.

The evaluations allow the OCTO SSR team to quantify training success in three areas:

- **Does our training clarify ICANN's role in investigations involving domain name system (DNS) or registration services?**
- **Does our training clarify the roles of generic top-level domain (gTLD) registry and registrar stakeholders in investigations involving DNS or registration services?**
- **Does our training give investigators a better understanding of how the Internet's system of unique identifiers and associated registration systems work?**

We believe that quantifying the answers to these questions is a "specific, measurable, achievable, relevant and time-oriented" (S.M.A.R.T.) means of measuring performance or success.

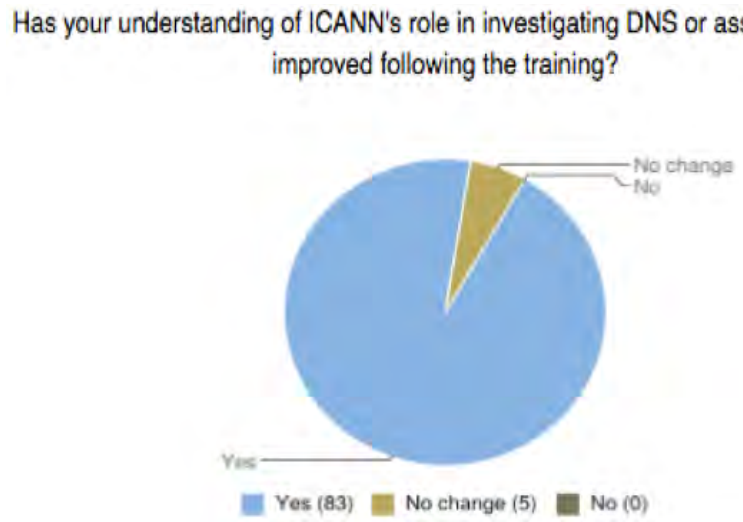
About Our Survey

OCTO team members do not take attendance during training. In some cases, the organizer takes attendance or requests contact information from trainees. In many training sessions, the attendance is fluid – e.g., drop-ins come for specific topics or attendees are called out to return to an in-progress investigation. Keeping these variables in mind, estimated total attendance for these eight events was between 160 and 180 trainees.

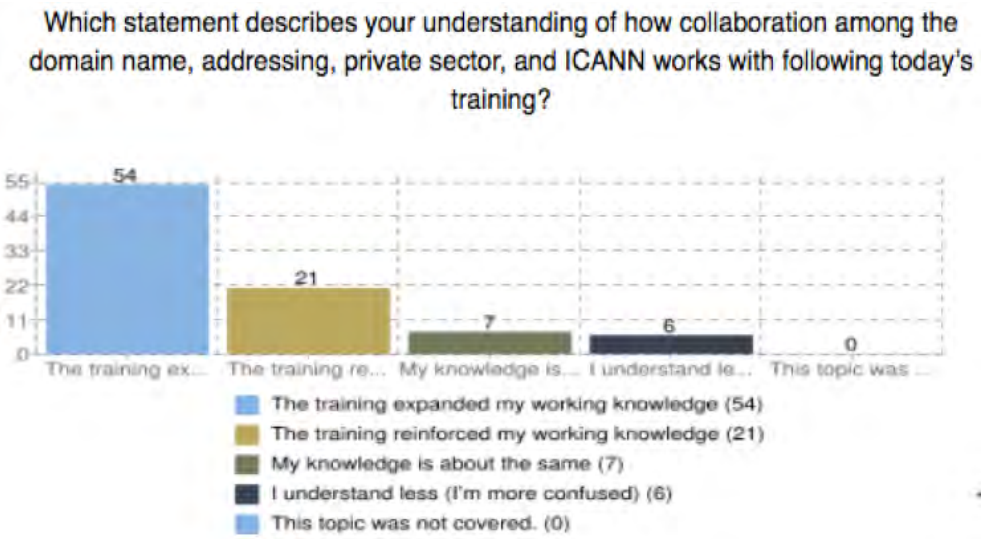
We use Jotform to process our online evaluations. We send an email, post a URL for trainees to visit after the class finishes, or we provide a printed version of the online form that attendees complete and return during the class. Our complete or partial (and usable) responses represent an approximate 49 to 56 percent response rate. This rate compares favorably with average response rates that are reported anecdotally for email surveys (SurveyGizmo, Fluidsurveys). More importantly, the sample is statistically valid. The numbers in the diagrams represent the raw data, not percentages.

Clarifying ICANN's Role in Investigations Involving the DNS

We asked two questions to measure the effectiveness of our training in clarifying ICANN's role in investigations involving the DNS. The responses from the seven training sessions in the measurement period suggest that the training program is effective. When asked if their understanding of ICANN's role in investigating the DNS or in assisting law enforcement officers had improved, 94 percent responded positively.

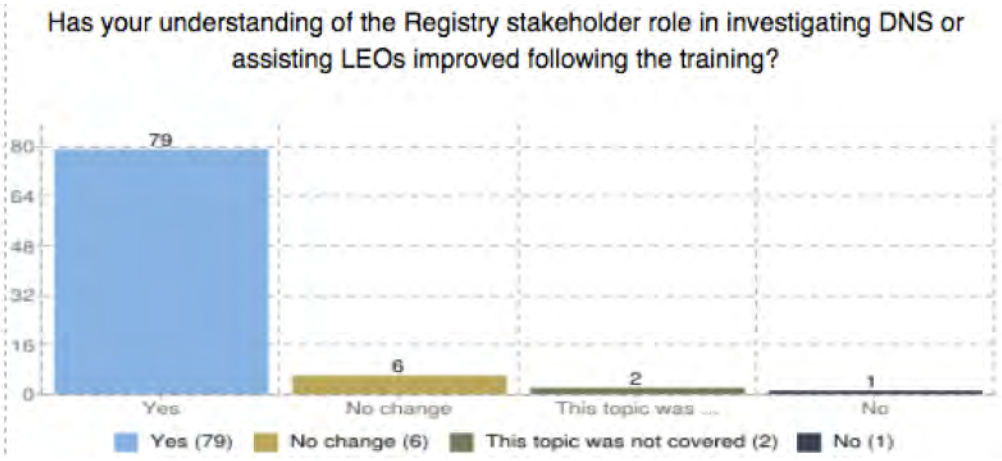


When asked to describe how the training affected their working knowledge of trust-based, multistakeholder collaboration, 61 percent of the trainees responded that their knowledge was expanded, and 85 percent responded that their working knowledge was expanded or reinforced.

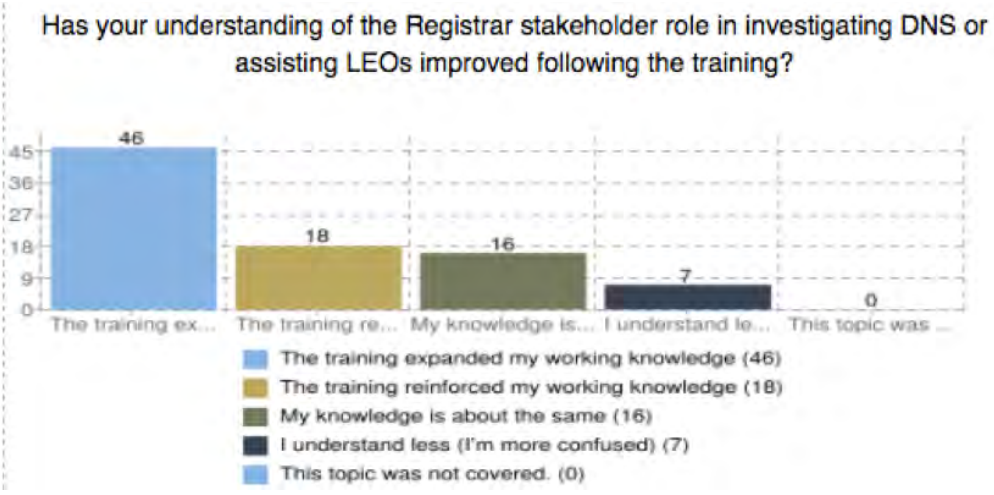


Clarifying Stakeholders' Roles in Investigations Involving the DNS

We ask two questions to measure our effectiveness in explaining the DNS ecosystem – DNS, gTLDs, country code TLDs (ccTLDs) and new TLD registries, registrars, registration service and content hosting providers. Explaining registry roles was very successful; 96 percent of trainees responded that their working knowledge expanded.



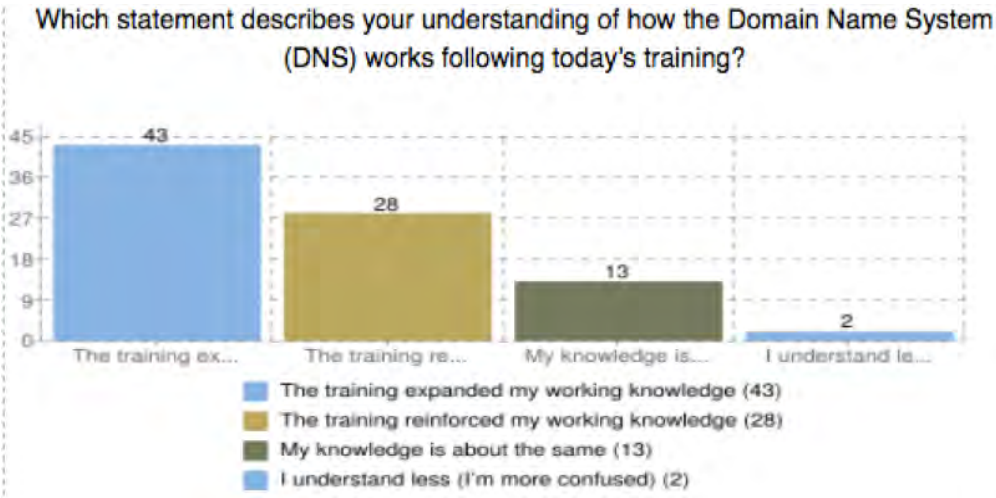
The responses regarding registrar roles indicate that 52 percent of trainees felt that their working knowledge had expanded. Another 39 percent responded that their working knowledge was reinforced or had remained the same.



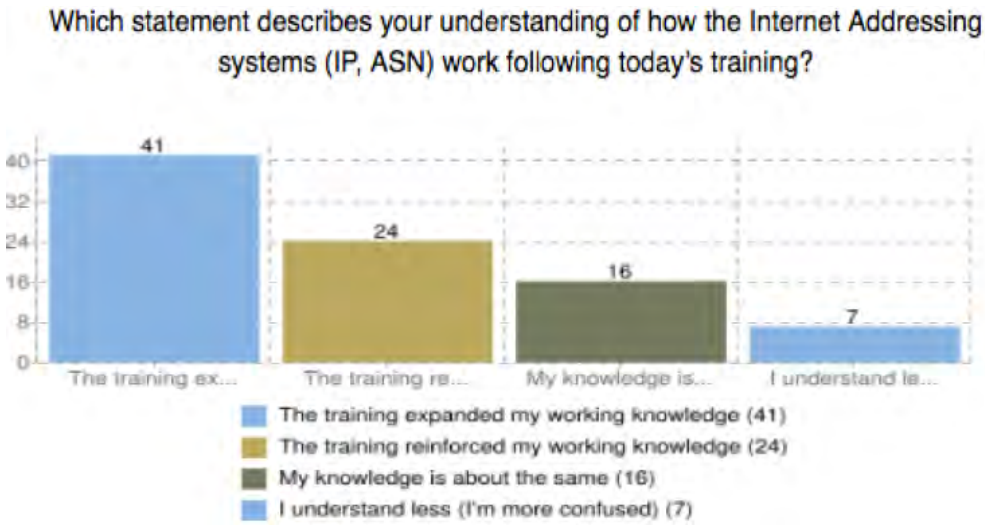
Educating Investigators on Technical Aspects of Identifier Systems

Providing opportunities for trainees to gain a better technical understanding of domain names, the DNS, Internet addresses and autonomous system numbers, and routing fundamentals is a priority for law enforcement agencies.

Our training expanded or reinforced the understanding of how the DNS works for 81 percent of our trainees.

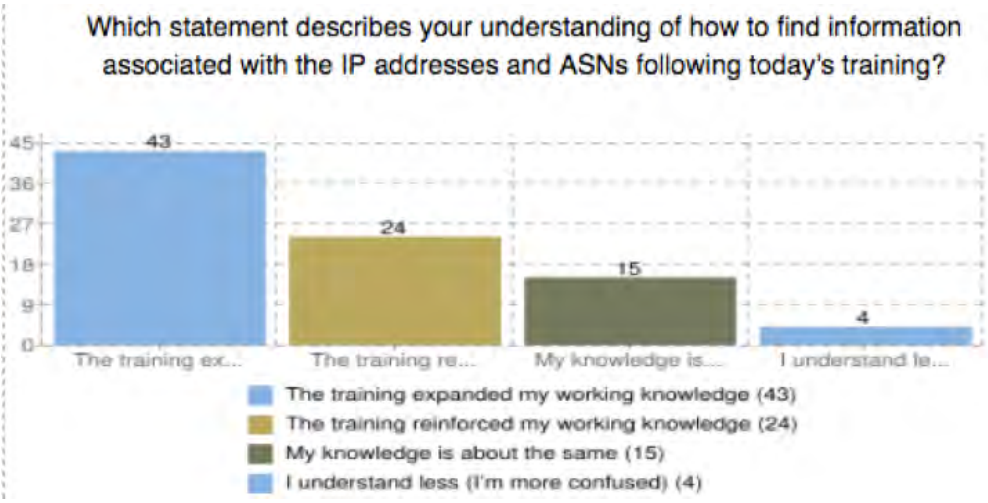


We expanded or reinforced the understanding of Internet numbering systems for 85 percent of our trainees.



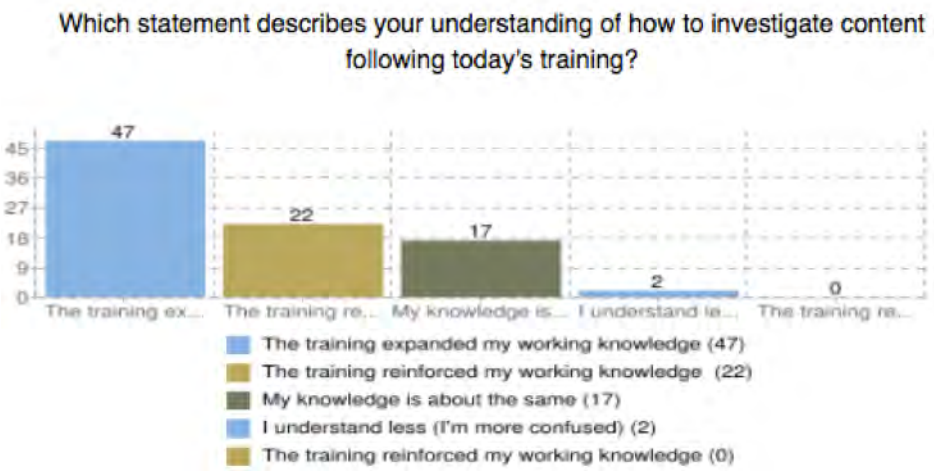
Collecting or Obtaining Internet Identifier Information

Investigators need to understand where to obtain information related to identifiers – and identifier system reputation data. When asked about their understanding of how and where to obtain information about Internet identifiers, 87 percent of trainees indicated that they had expanded or reinforced their understanding following the training.



Investigators must understand how to associate identifiers with hosted content or delivery services such as email and how to evaluate publicly available hosted content.

After the training, 78 percent of trainees indicated that they had expanded or reinforced their understanding of how to investigate content.



Current Assessment

The evaluations came from a diverse set of trainees in terms of nationality, experience, and (investigative) roles. Our training was intended to be neither introductory nor advanced, but rather to be applicable to participants with diverse backgrounds. The survey responses support anecdotal comments, and formal and informal correspondence received by the OCTO SSR team from public safety agencies or agents. The conclusion is that the training is effective and valuable for the intended audiences.

We asked about additional material that trainees would like to cover. The OCTO team will consider suggested topics for future iterations of the course material. This material changes regularly to keep pace with changes in cyberattacker or cybercriminal behavior and with the introduction or availability of new resources.

We also asked trainees for any general comments. A sample of these open-ended responses is presented below.

"Arrange training every quarter"

"Great training! Looking forward to an advanced training concerning this topic!"

"Thank you for the excellent training and the time you took for giving us an in depth view on how the stakeholders work together and investigation in cyberspace can be done. You work did shine a light on the possibilities and restrictions for Law Enforcement nowadays - the tools you provided us with will definitely find their way in our daily toolboxes."

"Thank you for the training, it was one of the most useful sessions I have been to over the last few years! Please do come back :-)"

"Lots of useful info and new tools tx"

"Thank you for excellent workshop. I was familiar with topic already, but training reinforced my knowledge. You also gave some tips that will help me in my line of work"

"I want to first say that it was very good training It expand my knowledge."

Appendix. Letters of Thanks

INTERNET DEVELOPMENT INITIATIVE

009/12-16

Dear David,

On behalf of Non-Governmental Organization "Internet Development Initiative - IDI", I would like to impress my gratitude for a training „Investigating DNS Abuse & Criminal use of the DNS" that was held through support of ICANN for law enforcement and other public structure representatives on December 5 and 7, 2016, in Tbilisi, Georgia.

The training was very productive and effective thanks to your highest qualification and professionalism as a trainer and a very positive personality.

All attendees of the training were extremely delightful about the importance of the training, highest professionalism of you as a trainer and your integrity towards your profession which was shown not only through your way of sharing training materials but also your attitude and profundity of explanation and support provided to each and every participant during the training sessions.

I hope our cooperation would become more fruitful and successful in the future.

I once again, thank you and wish you success in your endeavors.

I herein, would like to use this chance to thank ICANN for their support.

Sincerely,

Vladimer Svanadze

Chairmen of the Board

Info@indein.net +995 32 242 11 51 www.indein.net

Dear John

I wanted to personally say thank you to both Dave Piscitello and ICANN for the training that was provided to CERT-UK last Friday.

Clearly a busy week for him, and testimony to his commitment and drive that he spent his last day in the UK engaging with my analysts to present the DNS Investigations material. Feedback has been positive with the way the material was presented and well received by the analysts, especially the generously provided French patisserie - 'chouquettes'.

Recognising our role as the UK national CERT we welcome the opportunity to collaborate with and support ICANN in their outreach to law enforcement and other CERTs. The train the trainer aspect of our time with Dave is something we look forward to developing and specifically supporting Dave in delivering the material at ICDDF in March and independently beyond that to UK LE.

Best

Chris

Chris Gibson
Director, CERT-UK
e: cgibson@cert.gov.uk | t: +44 755 990 0200
pa: Hilary Morton | e: hmorton@cert.gov.uk | t: +44 207 147 4404
www: www.cert.gov.uk | twitter: @cert_uk

.BK

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

Klaus MITS, B.A., M.A.
LEITER DER ABTEILUNG II/BK
A-1014 WIEN
TEL: +43 1 [redacted]
FAX: +43 1 [redacted]
[redacted]
DVR: [redacted]

Vienna, 25 October 2016

Dear Mr Piscitello,

Following up on the positive feedback from the participants, it is my personal and sincere wish to thank you for the training you provided for our experts on the 28th September 2016. Today there is almost no criminal case without digital traces. Therefore knowledge about all kinds of indications that can result in new findings is of great importance.

Not only the high interest of our participants – many more applied for the training than we could accept – but also their feedback, that the presented information is a huge benefit for the day-to-day investigations, shows the significance and the high value of such trainings for our organisation.

So please let me thank you once more for you willingness to sharing your great knowledge and expertise, as well as your patience in answering all the questions of our investigators. Many thanks also to ICANN for giving our investigators the opportunity to attend the training free of charge. It would not be possible for us to get these important insights without this funding. We all hope, that we will be able to welcome you again in Vienna and that other investigators will also have the chance to deepen their knowledge in the future.

Yours sincerely,

Klaus Mits
Head of Department

BK.1 BUNDESMINISTERIUM FÜR INNERES

MINISTERIO DE RELACIONES EXTERIORES
DESPACHO VICEMINISTERIAL

Lima,

Mr. Goran Morby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers - ICANN
Los Angeles.-

It is my pleasure to express our congratulations for your nomination as the new Chief Executive Officer of the Internet Corporation for Assigned Names and Numbers (ICANN).

I also wish to extend our gratitude for the support received from ICANN, through the two DNS abuse and cyber-crime workshops held at the Ministry of Foreign Affairs this year. To this respect, I wish to highlight the splendid disposition of Mr. Carlos Alvarez, to make these opportunities possible and to further the experience through future workshops specially designed for the Pacific Alliance countries.

I would also like to reassure ICANN that Peru, will continue participating in the Governmental Advisory Committee through constructive perspectives on public policy issues and under a true multistakeholder spirit.

I take this opportunity to reiterate to you the assurances of my highest and most distinguished consideration.

Yours sincerely,

Eric Anderson Machado
Embajador
Encargado del Despacho Viceministerial
de Relaciones Exteriores

One World, One Internet

ICANN.ORG