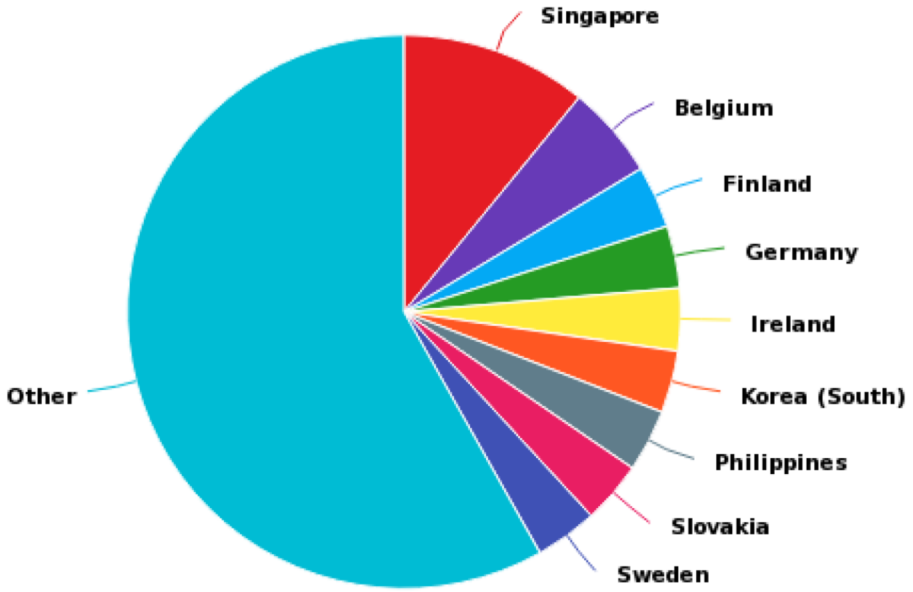
# RDS Law Enforcement Survey

## 1. Please indicate the country of your duty station:




| | | | |
|---|---|---|---|
| 1 - Singapore | 10.91% (6) | 2 - Belgium | 5.45% (3) |
| 3 - Finland | 3.64% (2) | 4 - Germany | 3.64% (2) |
| 5 - Ireland | 3.64% (2) | 6 - Korea (South) | 3.64% (2) |
| 7 - Philippines | 3.64% (2) | 8 - Slovakia | 3.64% (2) |
| 9 - Sweden | 3.64% (2) | 10 - Other | 58.18% (32) |

Response: 55

# Responses by Country

| | | | |
|---|---|---|---|
| Australia | 1 | Italy | 1 |
| Austria | 1 | Japan | 1 |
| Bahrain | 1 | Kenya | 1 |
| Belgium | 3 | Korea (South) | 2 |
| Brazil | 1 | Kuwait | 1 |
| Chile | 1 | Latvia | 1 |
| China | 1 | Mexico | 1 |
| Croatia | 1 | Morocco | 1 |
| Cyprus | 1 | Nigeria | 1 |
| Czech Republic | 1 | Philippines | 2 |
| Denmark | 1 | Singapore | 6 |
| Estonia | 1 | Slovakia | 2 |
| Finland | 2 | Slovenia | 1 |
| France | 1 | Sweden | 2 |
| Germany | 2 | Taiwan | 1 |
| Greece | 1 | Trinidad and Tobago | 2 |
| Hong Kong | 1 | United Kingdom | 1 |
| India | 1 | United States of America | 2 |
| Iran | 1 | Zambia | 1 |
| Ireland | 2 | Grand Total | 55 |

## 2. Please indicate your Unit/Department/Organization:

| | |
|---|---|
| 1 | cyber police |
| 2 | Investigation unit/ Cyber Crime Directorate/INTERPOL |
| 3 | Training Unit / Cybercrime Directorate / INTERPOL |
| 4 | Korean National Police Agency, Cyber Bureau |
| 5 | Cyber Crime Section/Economic and Financial Crimes Commission |
| 6 | Swedish National Police / Swedish Cyber Crime Centre |
| 7 | AFP ACSC Cybercrime |
| 8 | INTERPOL |
| 9 | General Directorate of Criminal Investigation \ CID and Licenses \ Arrest and follow up unit |
| 10 | NCA |
| 11 | Cybercrime Unit/National Criminal Police/Police and Border Guard Board |
| 12 | Internal Revenue Service |
| 13 | ZAMBIA POLICE SERVICE |
| 14 | National Police Agency |
| 15 | INTERPOL |
| 16 | National police, Cyber Crime Center |
| 17 | Computer investigation centre/Criminal police directorate/General Police directorate |
| 18 | Office for Combating Cybercrime / Crime Investigation Department / Cyprus Police |
| 19 | National Security Authority |

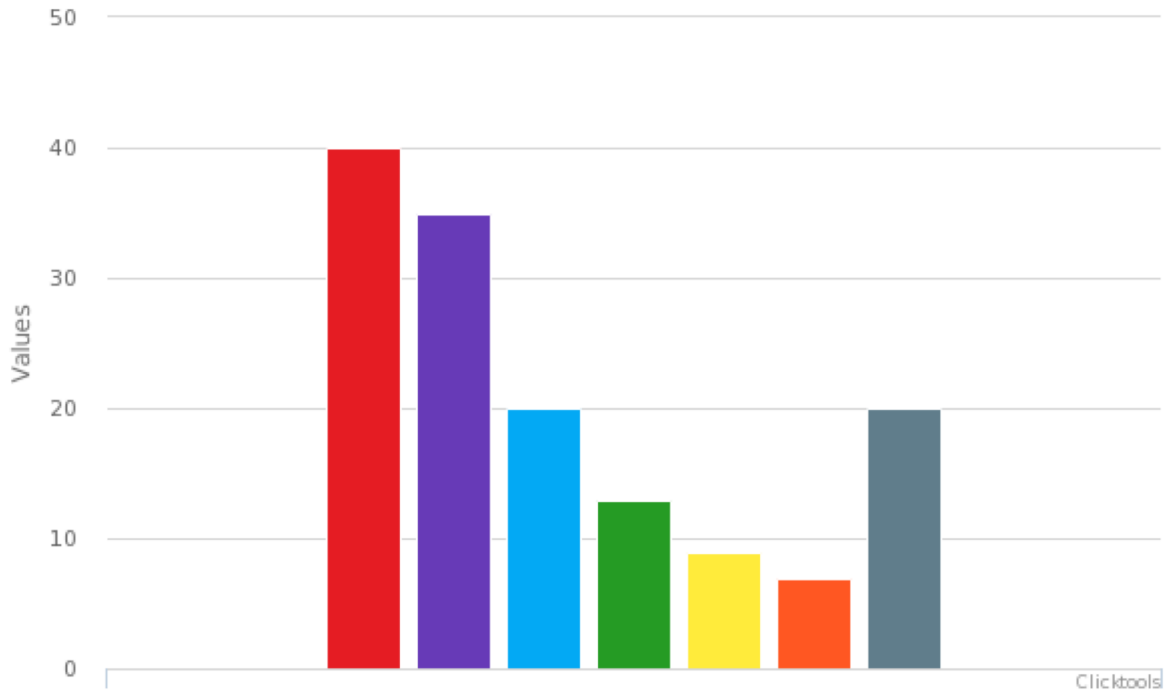
## 2. Please indicate your Unit/Department/Organization:

| | |
|---|---|
| 20 | Directorate of criminial Investigations |
| 21 | Cyber Crime Division, Police of the Czech Republic |
| 22 | Central Crime Department Lüneburg, Taskforce Cybercrime and digital Traces |
| 23 | 1st Unit (Operational cross-border cooperation (24/7) and SIS/SIRENE) International Cooperation Department Central Criminal Police Department State Police of Latvia |
| 24 | FNCCU |
| 25 | An Garda Siochana |
| 26 | SPF |
| 27 | IT Cyber Security |
| 28 | CNAIPIC/Polizia Postale e delle Comunicazioni/National Police |
| 29 | CYBER POLICE |
| 30 | Bundeskriminalamt Cybercrime Intelligence/Cybercrime Investigations |
| 31 | Federal Computer Crime Unit of the Federal Police |
| 32 | Belgian Federal Police - DJSOC |
| 33 | Federal Police |
| 34 | National Police |
| 35 | FBI Cyber Division |
| 36 | Cyber Crime Unit/Criminal Police Directorate/Ministry of Interior |
| 37 | Hong Kong Police Force |

## 2. Please indicate your Unit/Department/Organization:

| | |
|---|---|
| 38 | Cyber Unit /Scientific Division /Mexican Federal Police |
| 39 | MJIB Cyber Division |
| 40 | Kerala Police |
| 41 | National Bureau of Investigation / Cybercrime Center |
| 42 | Cybercrime Unit/Criminal Police Bureau |
| 43 | Department of Justice - Office of Cybercrime |
| 44 | Garda National Cyber Crime Bureau |
| 45 | Police of Finland / National Police Board |
| 46 | Cybercrime Division of Hellenic Police HQ |
| 47 | COMPUTER FORENSIC UNIT/NATIONAL INSTITUTE OF CRIMINALISTICS/BRAZILIAN FEDERAL POLICE |
| 48 | CyberCrimen Unit/PDI |
| 49 | CT |
| 50 | International Cooperation Team/Cyber Bureau/Korean National Police Agency |
| 51 | computer emergency incident response team |
| 52 | Philippine National Police |
| 53 | Cybercrime Intelligence/INTERPOL |
| 54 | Trinidad & Tobago Computer Security Incident Response Team (TTCSIRT) |
| 55 | Computer Security Incident Response Team |

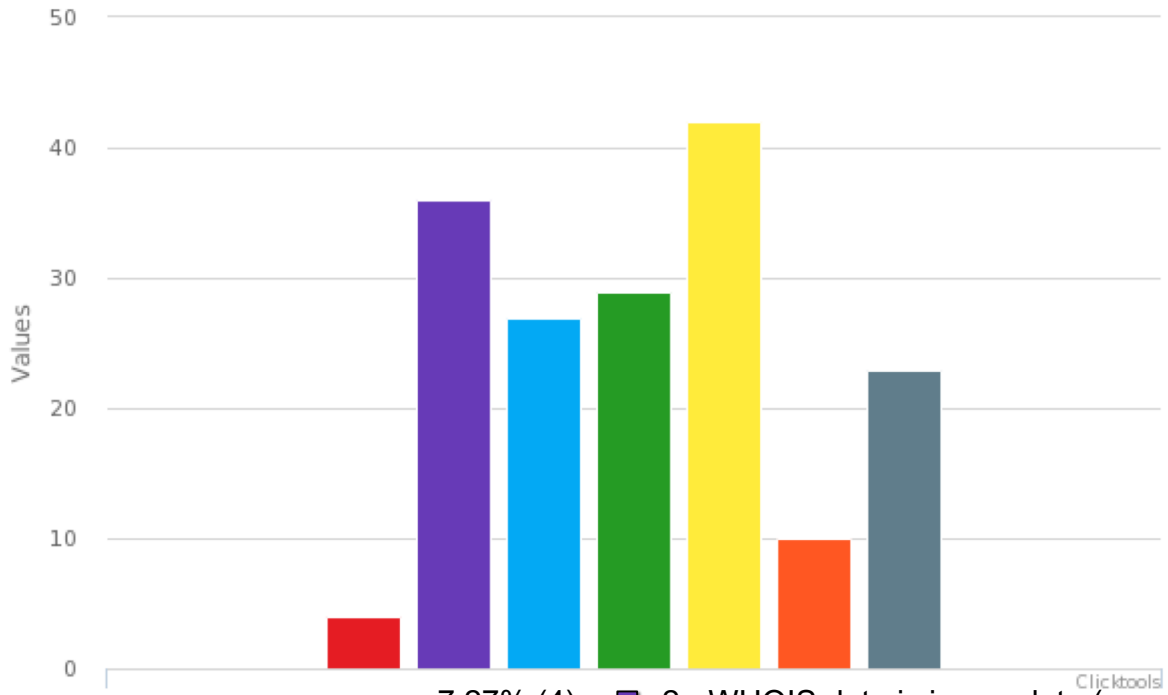
### 3. By which means do you or your agency look up WHOIS data?




| | | | |
|---|---|---|---|
| 1 - Third party commercial service, e.g. DomainTools | 72.73% (40) | 2 - ICANN WHOIS lookup portal (https://whois.icann.org/) | 63.64% (35) |
| 3 - The Internet's Network Information Center (InterNIC, https://www.internic.net/whois.html) | 36.36% (20) | 4 - Portal provided by Registrar, e.g. Godaddy | 23.64% (13) |
| 5 - Portal provided by Registry, e.g. Verisign | 16.36% (9) | 6 - Port 43 interface | 12.73% (7) |
| 7 - Other open source tools | 36.36% (20) | | |

Response: 55

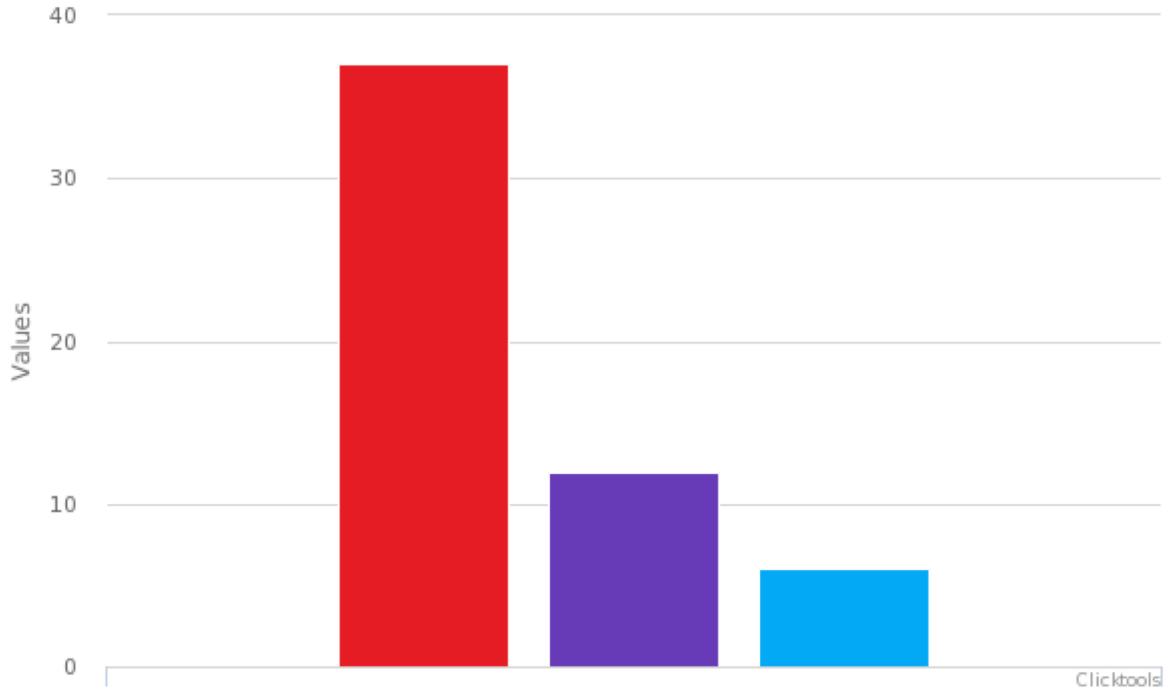
## 4. What are the issues you identified when using WHOIS data? (if any)




| | | | |
|---|---|---|---|
| 1 - No issues | 7.27% (4) | 2 - WHOIS data is incomplete (no registrant's email address and telephone number) | 65.45% (36) |
| 3 - WHOIS data is inaccurate, e.g. deliberately falsified | 49.09% (27) | 4 - Hard to tell whether the WHOIS data is accurate or not | 52.73% (29) |
| 5 - WHOIS data is protected by Privacy/Proxy service | 76.36% (42) | 6 - Inconsistent lookup results | 18.18% (10) |
| 7 - No central authority for WHOIS data lookup | 41.82% (23) | | |

Response: 55

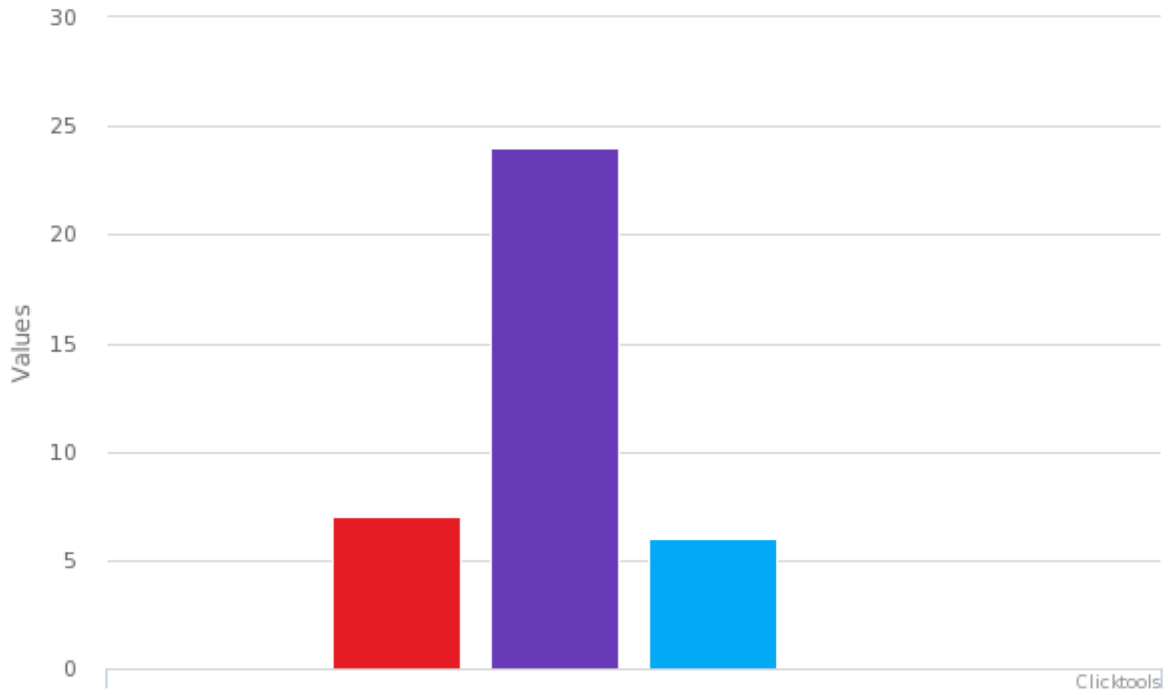
**5. Do you rely on third-party services provided by private companies in relation to WHOIS, e.g. DomainTools or others?**




| | | | |
|---|---|---|---|
| 1 - Yes | 67.27% (37) | 2 - No | 21.82% (12) |
| 3 - I don't know | 10.91% (6) | | |

Response: 55

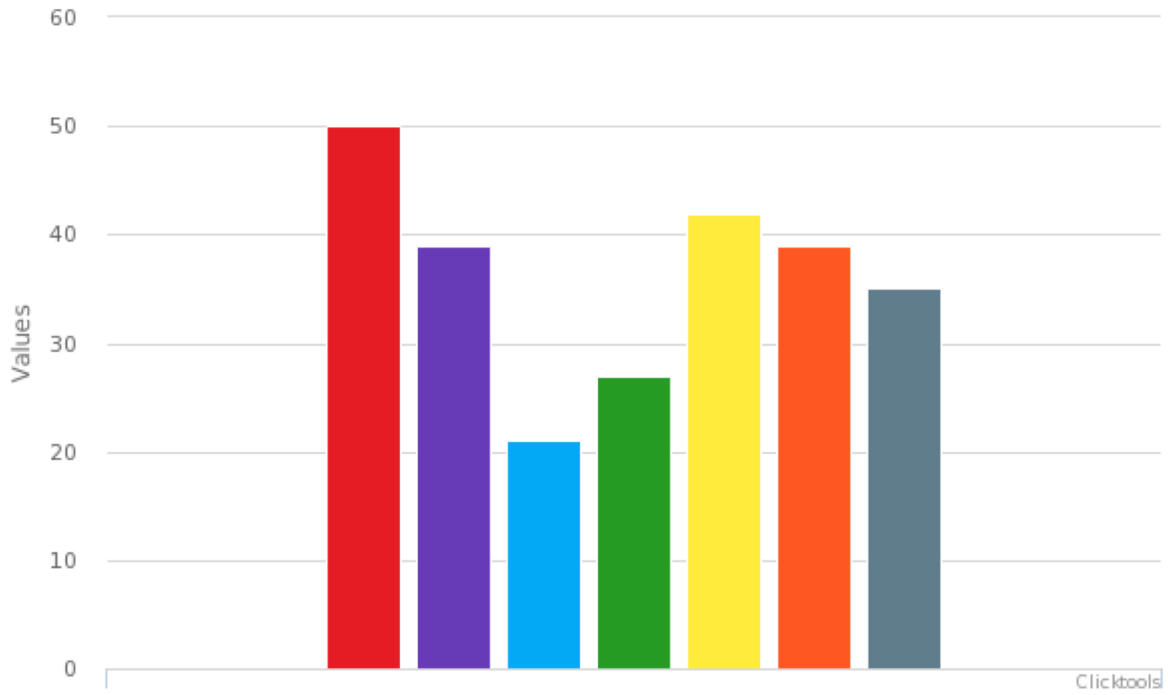
## 6. To what extent do you rely on these external services?




| | | | |
|---|---|---|---|
| 1 - For all lookups | 18.92% (7) | 2 - Frequently | 64.86% (24) |
| 3 - Occasionally | 16.22% (6) | 4 - Rarely | 0% (0) |

Response: 37

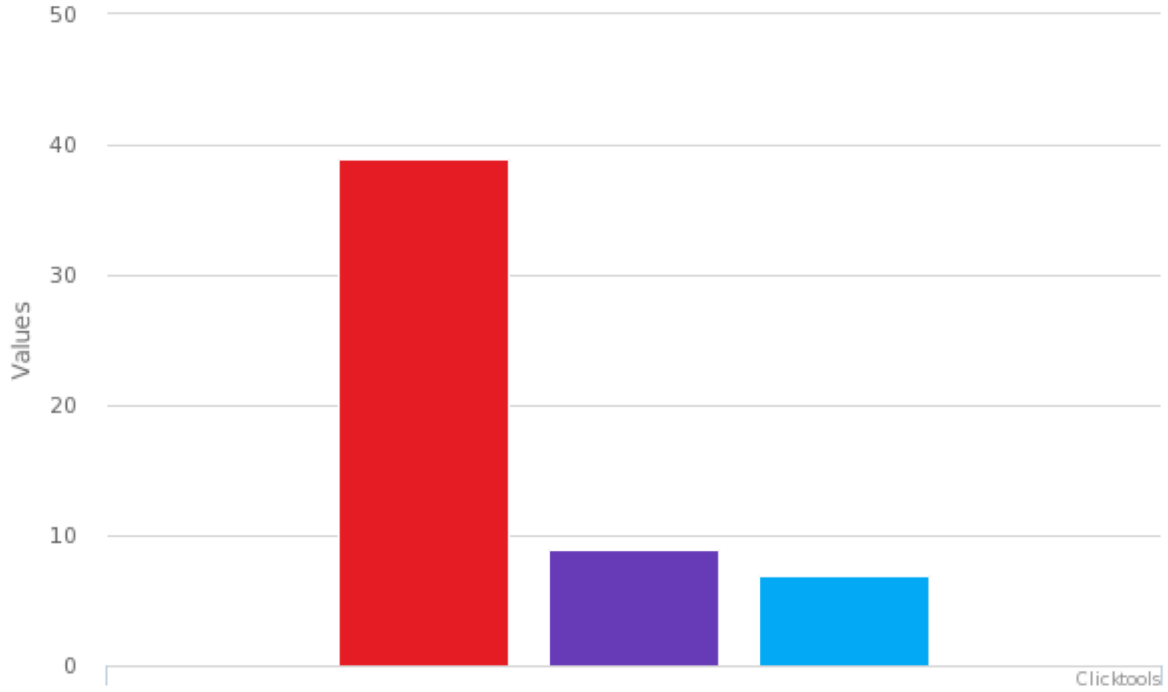
## 7. Which data fields do you rely on most or are most helpful to your investigation(s)?




| | | | |
|---|---|---|---|
| 1 - Registrant | 90.91% (50) | 2 - Admin | 70.91% (39) |
| 3 - Tech | 38.18% (21) | 4 - Billing | 49.09% (27) |
| 5 - Registrar | 76.36% (42) | 6 - Creation & updated date | 70.91% (39) |
| 7 - Name server and other related technical information (such as domain status) | 63.64% (35) | | |

Response: 55

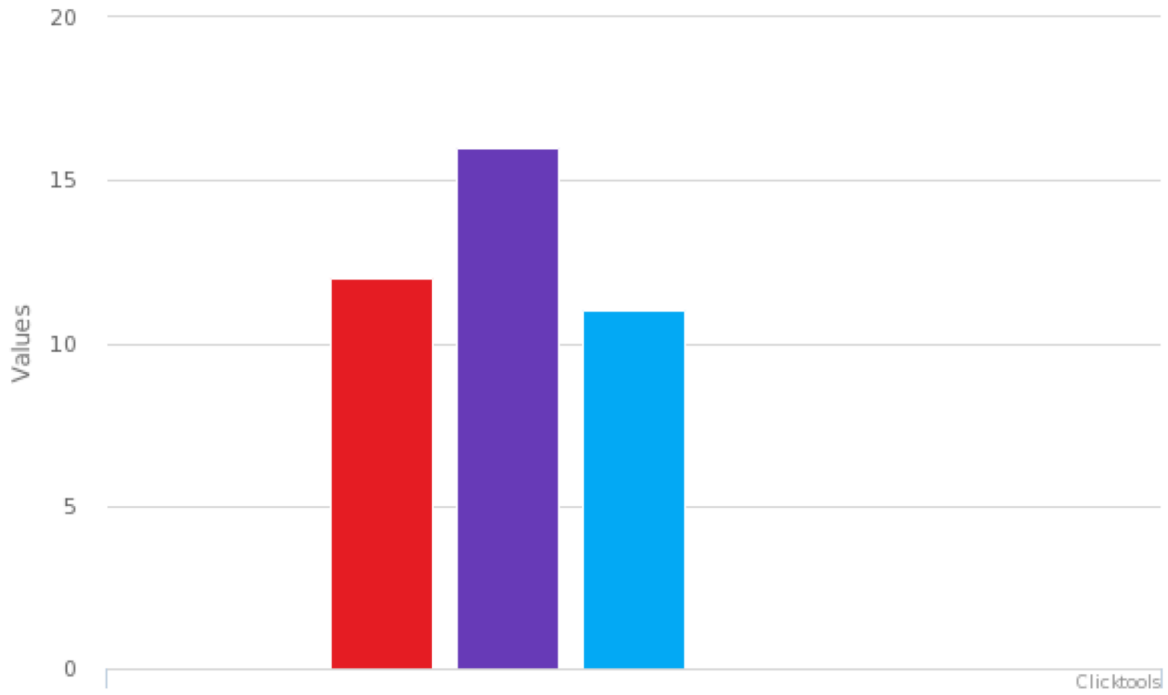
**8. Do you use cross-referencing/reverse lookup of WHOIS data fields, e.g. to identify other domains that were registered using the same information?**




| | | | |
|---|---|---|---|
| 1 - Yes | 70.91% (39) | 2 - No | 16.36% (9) |
| 3 - Not available | 12.73% (7) | | |

Response: 55

## 9. How often is this used?



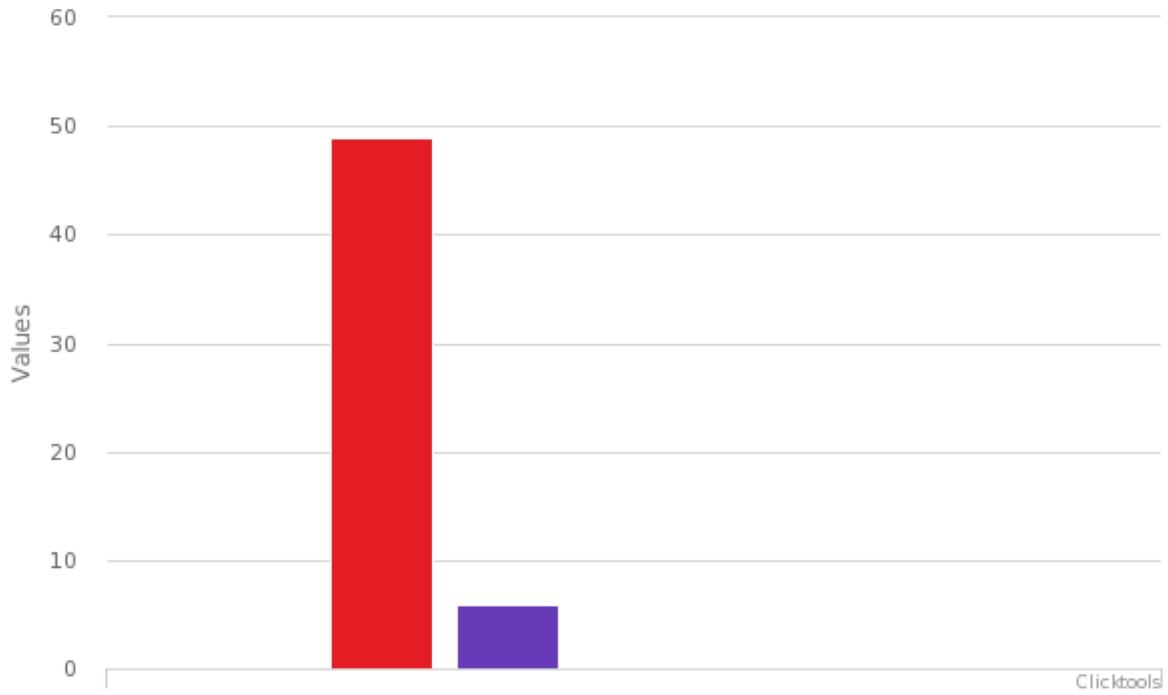

| | | | |
|---|---|---|---|
| 1 - Always or close to always | 30.77% (12) | 2 - Frequently | 41.03% (16) |
| 3 - From time to time | 28.21% (11) | 4 - Rarely | 0% (0) |
| 5 - Never or close to never | 0% (0) | | |

Response: 39

## 10. Please provide any comment(s) you may have on cross-referencing/reversed look-up.

| | |
|---|---|
| 1 | useful but needs improvement |
| 2 | usually the same |
| 3 | from emails provided on registration was same as that on another domain wedid not have before cross referenced look-up |
| 4 | https://mxtoolbox.com/ReverseLookup.aspx |
| 5 | Get IP by a Domain WHOIS, and Get other Domain(s) by the IP |
| 6 | All data not regulary updated or fake data provided |
| 7 | no comment |
| 8 | Help to identify other domains that were registered using the same information |
| 9 | This is an essetial investigative technique.  Pivoting off passive DNS (IP resolution) is critical to investigations as well. |
| 10 | N/A |
| 11 | It is a useful function to identify malicious domains |
| 12 | reverse lookup permits to find others related domains (from the original investigated) that incurrs for example in Phishing sites, malware spread, etc. |
| 13 | That's important to make sure "Do these domains belong to the same group/person?", to identify the DNS abuse problem. |
| 14 | Helpful for comprehensive investigations |
| 15 | Sometimes Information is a match |
| 16 | This is critical in buidling LEA relevant intellgence on threat actors. Using diferent seed data provides oppurunities to locate further indicators which have degrees of sepearation. |

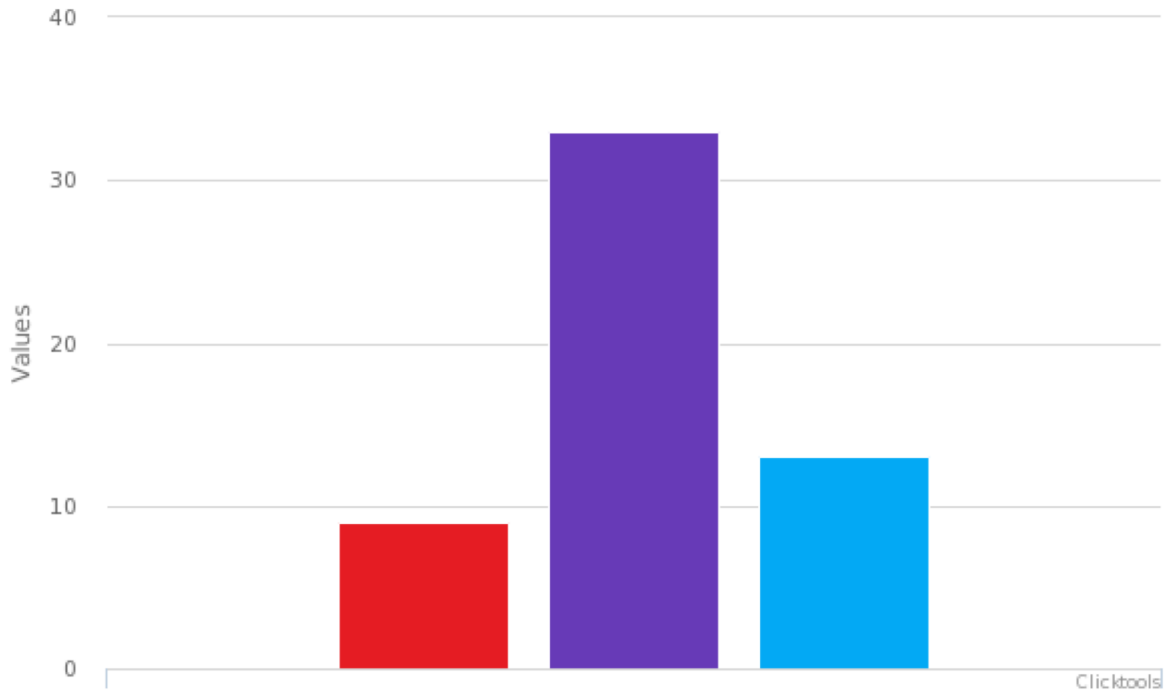
## 11. How important is WHOIS for law enforcement activities?




| | | | |
|---|---|---|---|
| 1 - Very important | 89.09% (49) | 2 - Important | 10.91% (6) |
| 3 - Neutral | 0% (0) | 4 - Not very important | 0% (0) |
| 5 - Unimportant | 0% (0) | | |

Response: 55

**12. Are there alternative data sources that you could use or already use to fulfill the same investigative needs?**



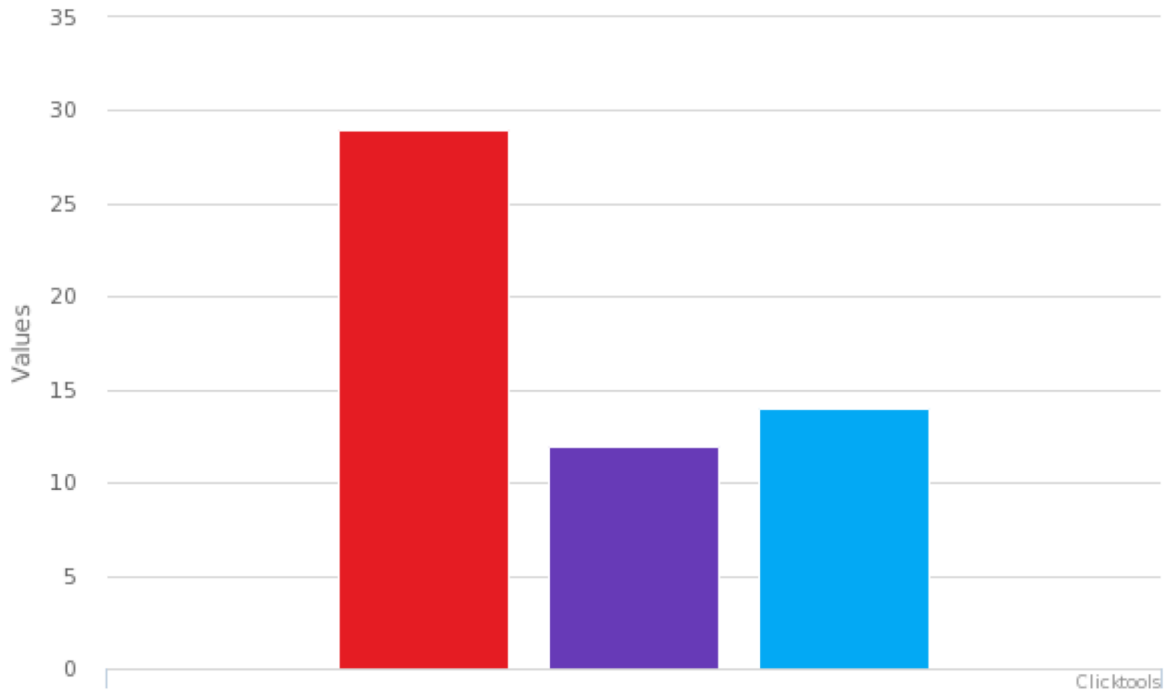

| | | | |
|---|---|---|---|
| 1 - Yes | 16.36% (9) | 2 - No | 60% (33) |
| 3 - I don't know | 23.64% (13) | | |

Response: 55

## 13. Which data source(s) do you or could you use alternatively?

| | |
|---|---|
| 1 | The INTERNET |
| 2 | domaintools reverse lookup from our state department in lower saxony |
| 3 | Robtex |
| 4 | Subscriber check from ISP check |
| 5 | Internal Databases from historic investigations. |
| 6 | https://centralops.net,www.misk.com/tools/#dns |
| 7 | JsonWhois WhoisAPI |
| 8 | In some cases: ISP |
| 9 | ViewDNS, Domain history |

**14. Have you come across any issues when requesting data behind privacy and proxy services in your use of the WHOIS?**




| | | | |
|---|---|---|---|
| 1 - Yes | 52.73% (29) | 2 - No | 21.82% (12) |
| 3 - I don't know | 25.45% (14) | | |

Response: 55

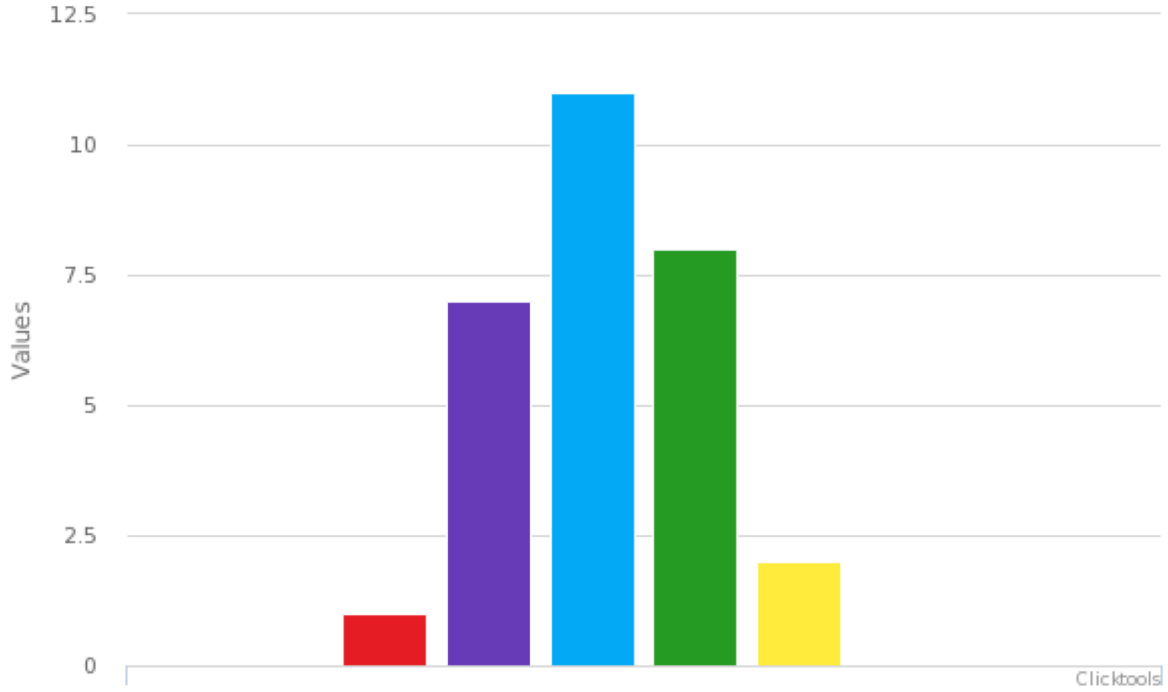
## 15. If yes, please specify below

| | |
|---|---|
| 1 | On requesting for certain domains registered at some specific coroprations, all nformation is protected due to proxy or privacy reasons. |
| 2 | Criminal exploit those service protect their identity. |
| 3 | No help given |
| 4 | privacy companies |
| 5 | Usually the request will be denied as it is located out of our jurisdiction, and taking too much processing time to go through MLA process |
| 6 | Unable to obtain data in a timely manner and / or unacceptable risk to opertion due to probability of notification. |
| 7 | We rarely received a response when we contact someone using privacy or proxy services. |
| 8 | Investigations are hampered due to a lot of paper work and legal instruments to access that data sort |
| 9 | onamae.com |
| 10 | The proxy company doesn't want to give the data, as they offer privacy as a service to their users |
| 11 | No answers |
| 12 | Law obstacles |
| 13 | e.g. informations held by registrars out of the Czech Republic |
| 14 | can't access data and no response using the proxy service |

## 15. If yes, please specify below

| | |
|---|---|
| 15 | Some data is hidden and unavailable |
| 16 | Unfortunatly many of poxy services doesnot cooperat |
| 17 | They are usually situated in foreign countries. Therefor an international letter of request needs to be sent, which is very time consuming. |
| 18 | No information |
| 19 | It takes too long to get the data. They become obsolete. |
| 20 | Specifically if the privacy/proxy service is not operated out of the United States. Also, cross-referencing/lookups to identify other infrastructure becomes moot. |
| 21 | In most cases an MLAT is needed and it takes time to get the information. |
| 22 | Cross-jurisdiction issues if the privacy or proxy services is situated in overseas |
| 23 | Proxy services are reluctant to collaborate with law enforcement of potential culprits. Because their bussines models are not oriented to support the public safety in the Internet. |
| 24 | No data available or gdpr masked. |
| 25 | Usually these companies delay answers or they do not respond at all or local Authorities demand cumbersome MLATs (Mutual Legal Assistance Treaty) |
| 26 | SOMETIMES THE INFORMATION IS OUT OF MY COUNTRY AND WE NEED COOPERATION AGREEMENTS WITH THE OTHERS COUNTRIES. |
| 27 | We can´t see all the information we were used to see. |
| 28 | Identy can't be specified. No further investigations possible or difficult. |

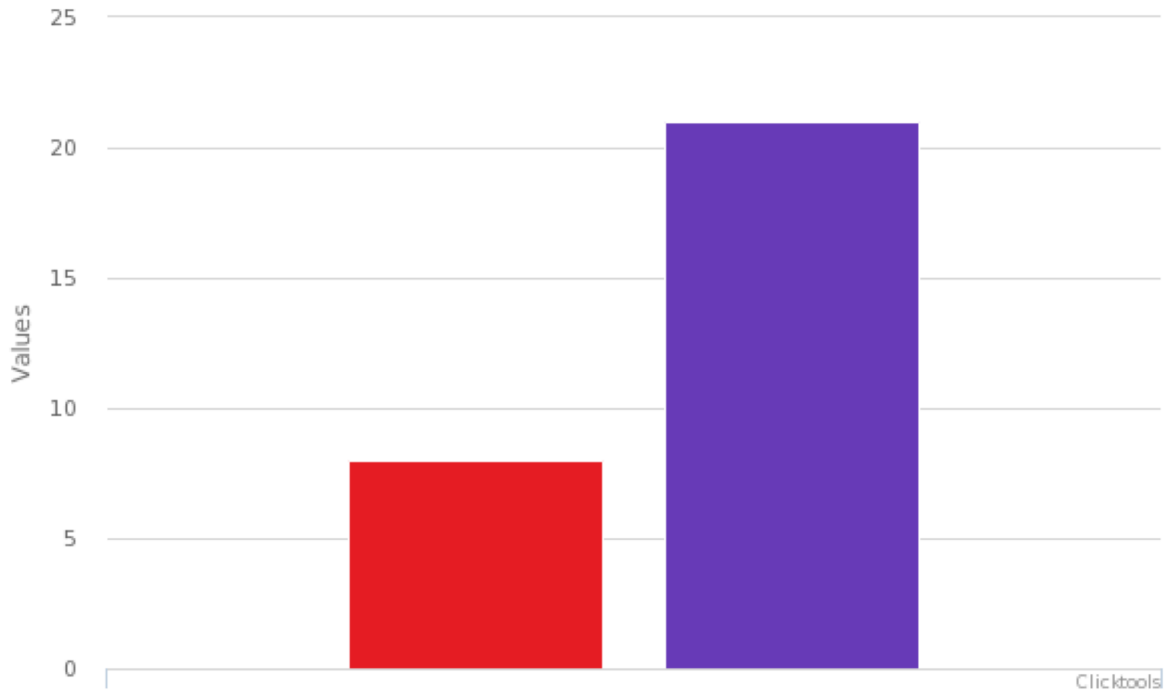
**16. In what percentage of lookups (approximately) do you encounter privacy/proxy services?**




| | | | |
|---|---|---|---|
| 1 - 0-10% | 3.45% (1) | 2 - 10-20% | 24.14% (7) |
| 3 - 20-40% | 37.93% (11) | 4 - 40-60% | 27.59% (8) |
| 5 - 60-80% | 6.9% (2) | 6 - 80-100% | 0% (0) |

Response: 29

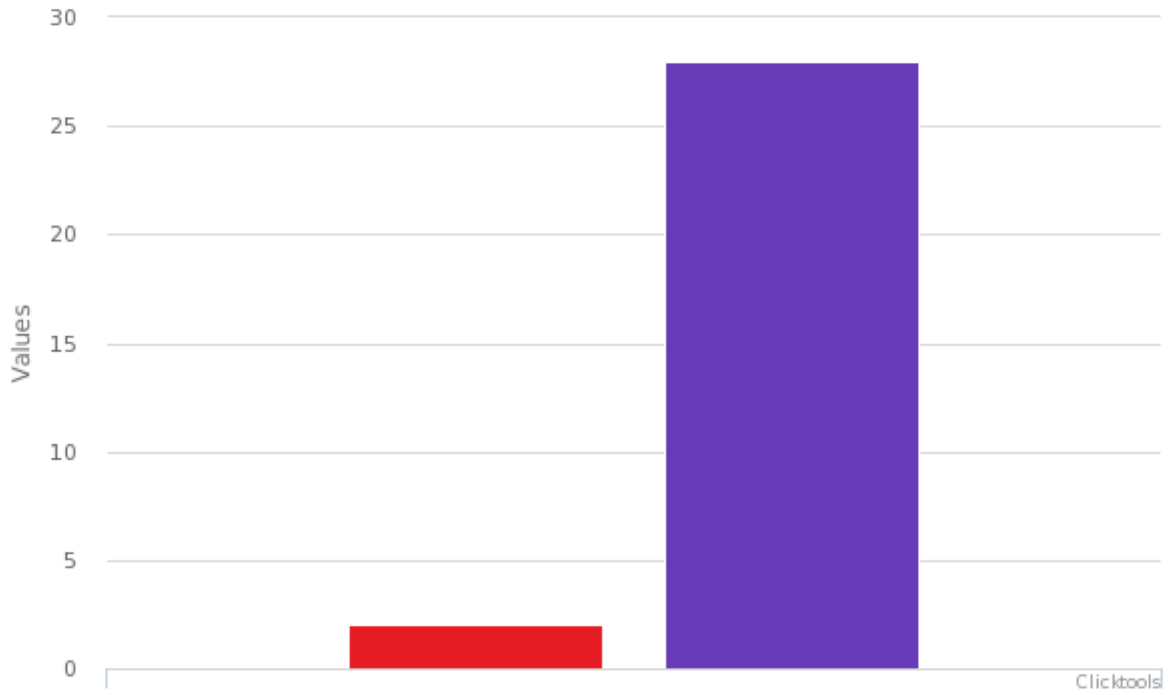
## 17. Were you able to obtain data on the registrant?




| | | | |
|---|---|---|---|
| 1 - Yes | 27.59% (8) | 2 - No | 72.41% (21) |

Response: 29

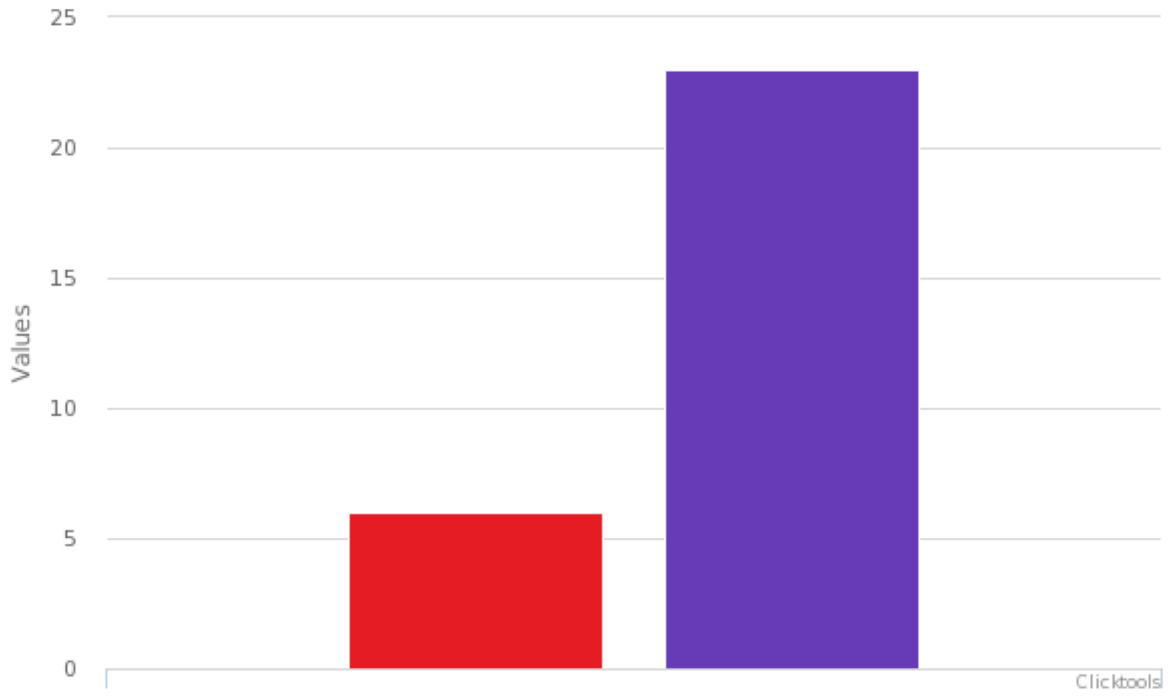
## 18. Did cooperation with the privacy/proxy service function well?




| | | | |
|---|---|---|---|
| 1 - Yes | 6.9% (2) | 2 - No | 96.55% (28) |

Response: 29

**19. Was the data obtained in time to allow the investigation to proceed?**




| | | | |
|---|---|---|---|
| 1 - Yes | 20.69% (6) | 2 - No | 79.31% (23) |

Response: 29

**20. Do you have experience using gated access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation?**

| | |
|---|---|
| 1 | no experience on gated access systems yet |
| 2 | No |
| 3 | None |
| 4 | No |
| 5 | DomainTools |
| 6 | No |
| 7 | No |
| 8 | Yes, signed Organisation agreement to access gated data |
| 9 | Yes, we have used different gated systems. The system should be over encrypted channel and have reasonable password or certification policy. |
| 10 | Yes |
| 11 | NO |
| 12 | Yes, we do. Just to declare we are National Police Agency. |
| 13 | no |
| 14 | No |
| 15 | no direct access |

**20. Do you have experience using gated access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation?**

| | |
|---|---|
| 16 | No |
| 17 | No, but good API type access would be very efficient for us |
| 18 | No |
| 19 | No |
| 20 | Yes, with domaintools. Requirements should be: free or cheap access, API-Interface |
| 21 | No |
| 22 | yes.Dedicated platform was built and protocol for sharing data/voluntary disclosure signed with private companies |
| 23 | No |
| 24 | Don't know. |
| 25 | No |
| 26 | NO |
| 27 | yes some internal data base. |
| 28 | Gated access could be problematic due to sovereignty principles (government would nedd to allow access) if it's not being provided by one central authority (e.g. ICANN). |
| 29 | No |
| 30 | No |

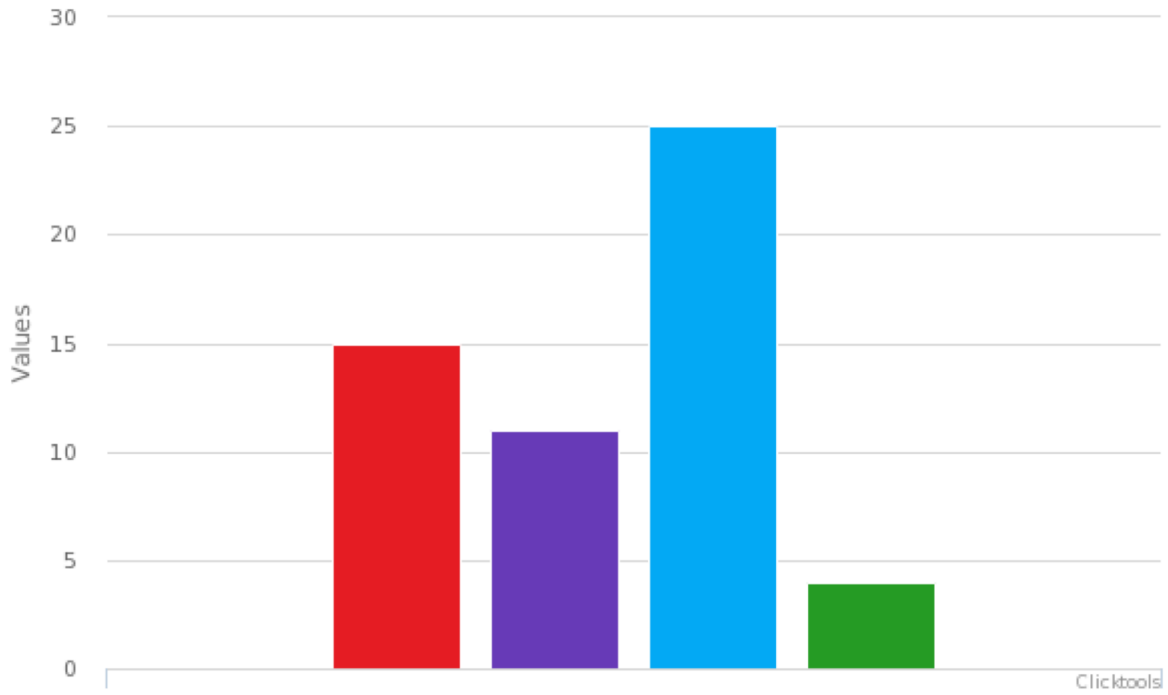
**20. Do you have experience using gated access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation?**

| | |
|---|---|
| 31 | No |
| 32 | No |
| 33 | Yes |
| 34 | No. |
| 35 | Yes, for subscribed services of private sector products |
| 36 | Regarding the security management of personal and institutional information, we have implemented the ISO27001 (we renewed this certification for 2017) to manage the information confidentiality, availability and integrity. |
| 37 | Of course, like account ,password ,OTP ,2-factor authentication. |
| 38 | Several cases we can get the basic information |
| 39 | No, requirements haven't been defined. |
| 40 | Yes we do. Requirements depends on the level of security for concrete access system. (e.g. minimum length of password, complexity of password, password expiration period, security certificate, security token, etc.) |
| 41 | email, computer and vpn access |
| 42 | No |
| 43 | Yes. Reliability, security. |
| 44 | Yes. My organisation uses only strict credentials and security policies to access systems and computational resources |

**20. Do you have experience using gated access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation?**

| | |
|---|---|
| 45 | YES, SIGNS TERM OF COMMITMENT AND RESEARCH |
| 46 | we don´t have credentials assigned |
| 47 | Yes |
| 48 | No |
| 49 | We do have experience of gated access systems and we do have credentials assigned for every personnels |
| 50 | None |
| 51 | Yes |
| 52 | No |
| 53 | No |

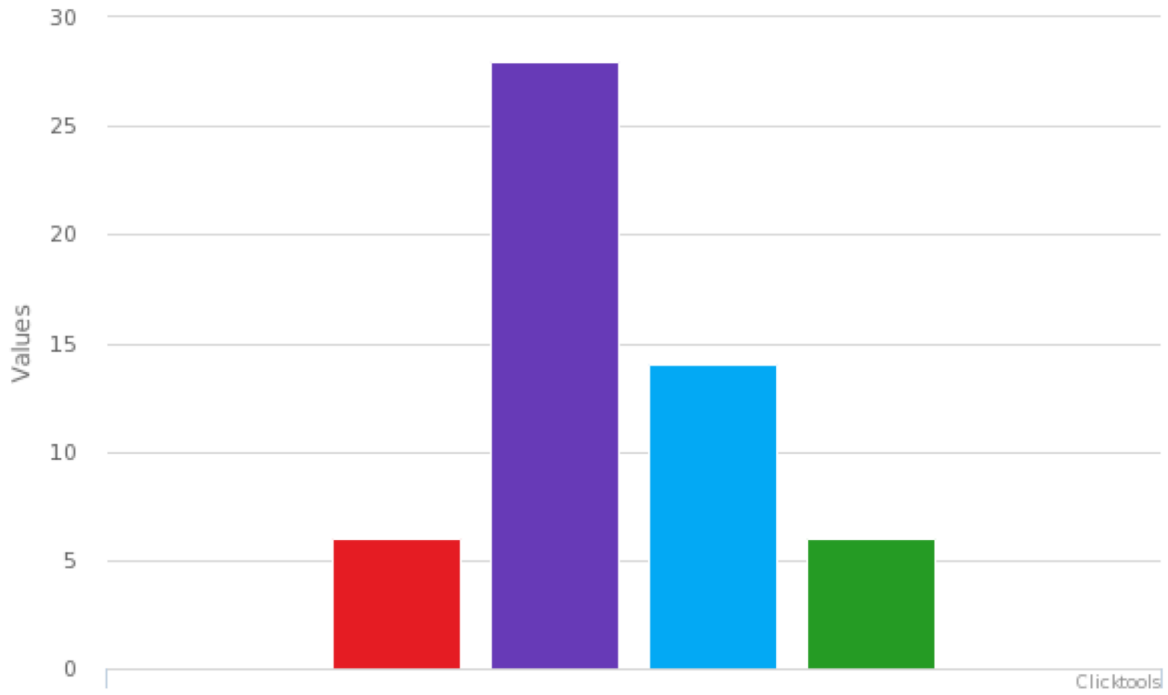
**21. Where WHOIS access to the name and address of the registrant is discontinued, how would you conduct your investigations?**




| | | | |
|---|---|---|---|
| 1 - By going to the ISPs | 27.27% (15) | 2 - By relying on direct cooperation with registrars and registries on the basis of a request form or other individualized request | 20% (11) |
| 3 - By obtaining a legal instrument and going to the registrars or registries | 45.45% (25) | 4 - Other means (Please explain) | 7.27% (4) |

Response: 55

**22. Where WHOIS information is not available on a public query basis, how does this usually affect an investigation?**



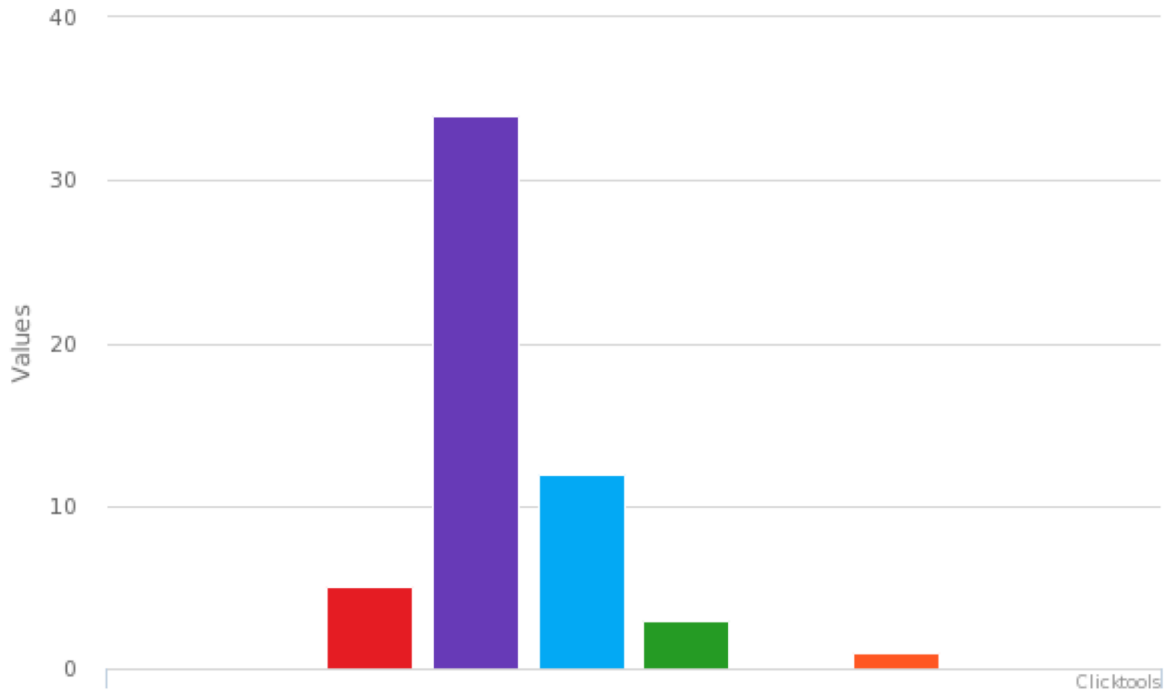

| | | | |
|---|---|---|---|
| 1 - Other means are pursued | 11.11% (6) | 2 - The investigation is delayed | 51.85% (28) |
| 3 - The investigation is discontinued | 25.93% (14) | 4 - Other (please explain) | 11.11% (6) |

Response: 54

## 23. Please specify if possible:

| | |
|---|---|
| 1 | look at other avenues of investigation |
| 2 | If it's possible, history data would be fine. |
| 3 | Legal instruments |

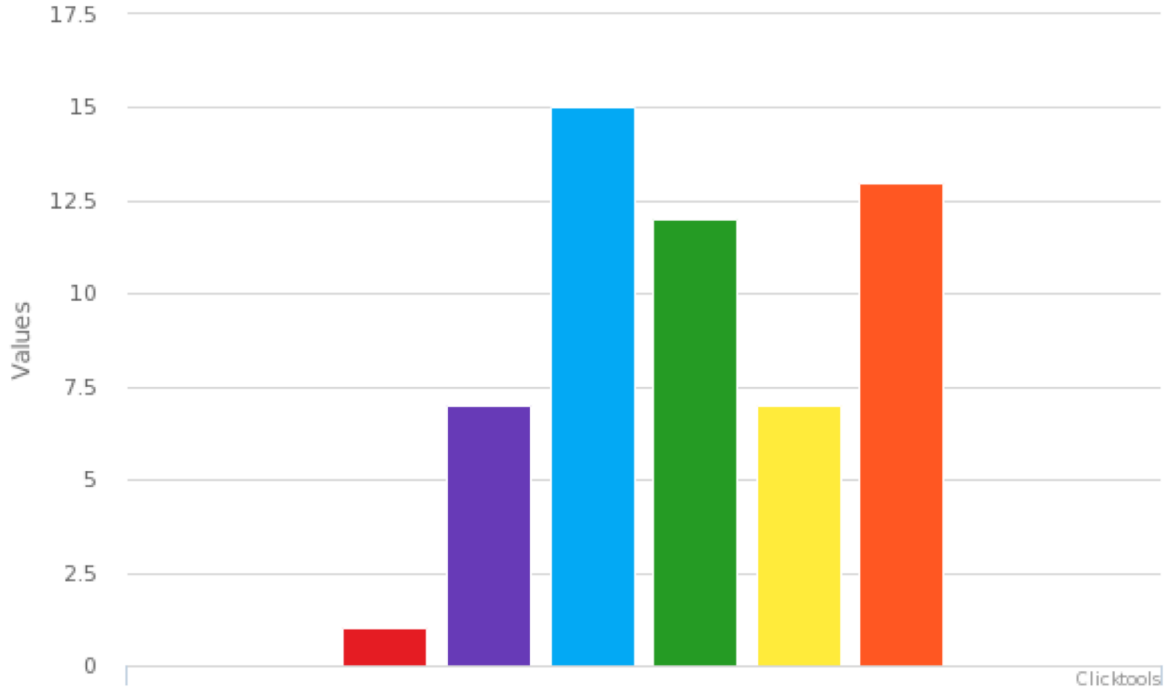
## 24. Prior to May 2018, how many WHOIS lookups did you personally make per month?




| | | | |
|---|---|---|---|
| 1 - <10 | 9.09% (5) | 2 - Between 10 and 100 | 61.82% (34) |
| 3 - Between 100 and 1000 | 21.82% (12) | 4 - Between 1000 and 10000 | 5.45% (3) |
| 5 - >10000 | 0% (0) | 6 - None | 1.82% (1) |

Response: 55

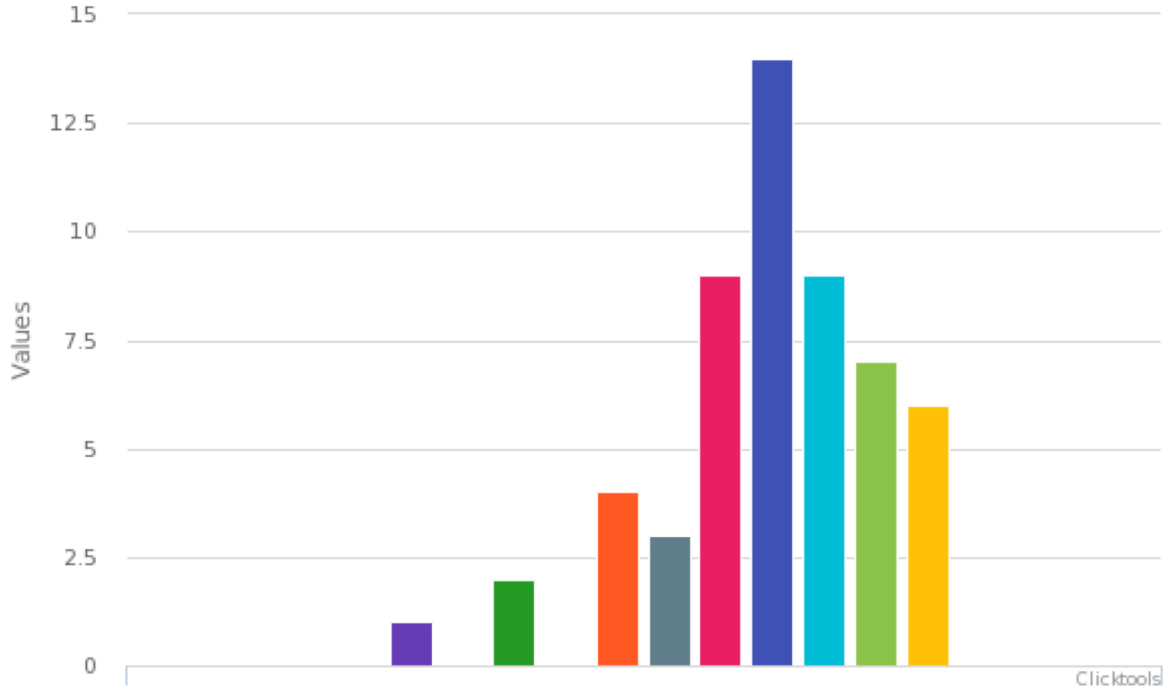
**25. Prior to May 2018, how many lookups did your unit or other units or agencies in your jurisdiction whose use you are aware of make?**




| | | | |
|---|---|---|---|
| 1 - <10 | 1.82% (1) | 2 - between 10 and 100 | 12.73% (7) |
| 3 - between 100 and 1000 | 27.27% (15) | 4 - between 1000 and 10000 | 21.82% (12) |
| 5 - >10000 | 12.73% (7) | 6 - I don't know | 23.64% (13) |

Response: 55

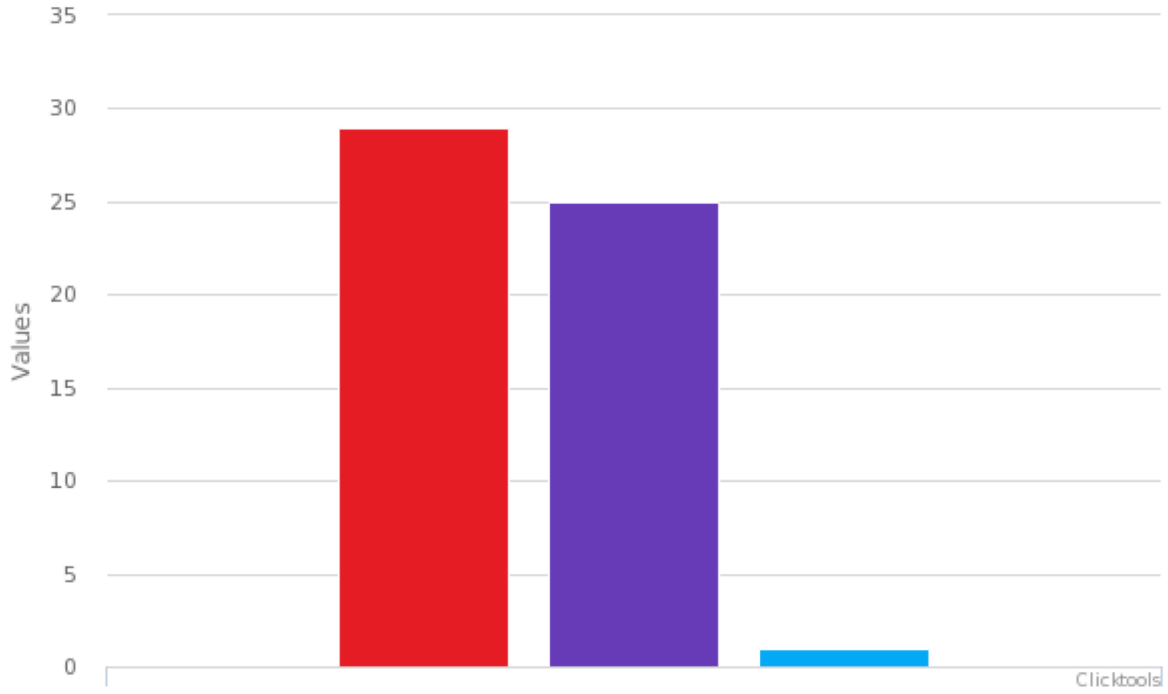
**26. Prior to May 2018, what was the percentage of WHOIS lookup results, generally speaking, that helped your investigation?**




| | | | |
|---|---|---|---|
| 1 - <10% | 0% (0) | 2 - 10% | 1.82% (1) |
| 3 - 20% | 0% (0) | 4 - 30% | 3.64% (2) |
| 5 - 40% | 0% (0) | 6 - 50% | 7.27% (4) |
| 7 - 60% | 5.45% (3) | 8 - 70% | 16.36% (9) |
| 9 - 80% | 25.45% (14) | 10 - 90% | 16.36% (9) |
| 11 - 100% | 12.73% (7) | 12 - I don't know | 10.91% (6) |

Response: 55

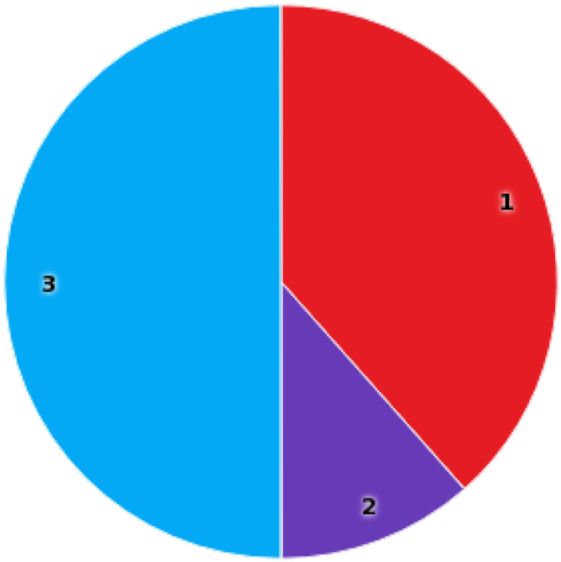
**27. Prior to May 2018, did the WHOIS lookup functionality (anonymous & public access) meet your needs for the purposes of law enforcement investigations?**




| | | | |
|---|---|---|---|
| 1 - Yes | 52.73% (29) | 2 - Partially | 45.45% (25) |
| 3 - No | 1.82% (1) | | |

Response: 55

## 28. Prior to May 2018, how did it not meet your needs?




Clicktools

| | | | |
|---|---|---|---|
| 1 - Inaccurate data | 38.46% (10) | 2 - No data available | 11.54% (3) |
| 3 - Other | 50% (13) | | |

Mean: 2.12
Response: 26

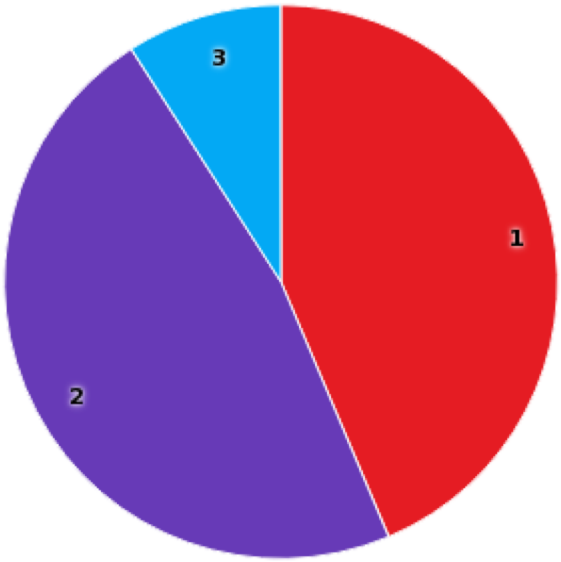
**29. Please specify in what way the WHOIS did not meet your needs.**
**Please specify whether your answer refers to your unit or also includes other units or agencies.**

| | |
|---|---|
| 1 | just personal experience: contact information especially address and telephone is usually inaccurate and sometimes the email address is not even valid. |
| 2 | Inaccurate data as well as privacy protected data |
| 3 | No reverse lookups by default. |
| 4 | The data tended to be inaccurate, but at the same time being inaccurate helped finding patterns. Also, there was no good way of fetching information automatically through an API. |
| 5 | also other organization units in the public administration |
| 6 | more information about the registrar with phone and mail addresses |
| 7 | Inaccurate data |
| 8 | Inaccurate information |
| 9 | lack of information (billing, payment, change log, IP used to register the domain, IP used to make change to registration) inaccurate data. The answare also include other units and agencies |
| 10 | see answer to question 28 |
| 11 | Falsified information |
| 12 | incomplete information, incorrect information |
| 13 | Proxies - Unit |

**29. Please specify in what way the WHOIS did not meet your needs.**
**Please specify whether your answer refers to your unit or also includes other units or agencies.**

| | |
|---|---|
| 14 | falsified/inaccurate/incomplete data still presented challenges prior to May 2018. |
| 15 | Sometimes the location of the IP address is incorrect, sometimes the information is blocked by guarding services (referring to my unit) |
| 16 | When we check WHOIS information, find no such street in real.My answer refers to my unit. |
| 17 | Some cases, wrong email Ids |
| 18 | general info and/or privacy protected |
| 19 | Some of the data is reliable as it is not verified during registration |
| 20 | Available data was inaccurate as it is not sufficiently verified. Answer refers to Finnish Police. |
| 21 | Mostly privacy-proxy services |
| 22 | MY UNIT - POOR QUALITY AND LOW INFORMATION |
| 23 | Anwser 28 |
| 24 | We had limitations in obtaining the IP address of the registrant |
| 25 | no data available |
| 26 | From an intelligence building perspective privacy protect service created a deadend lead. Of course an universal KYC would greatly improve the reliabilty of the database |

## 30. Has your usage of WHOIS changed since May 2018?

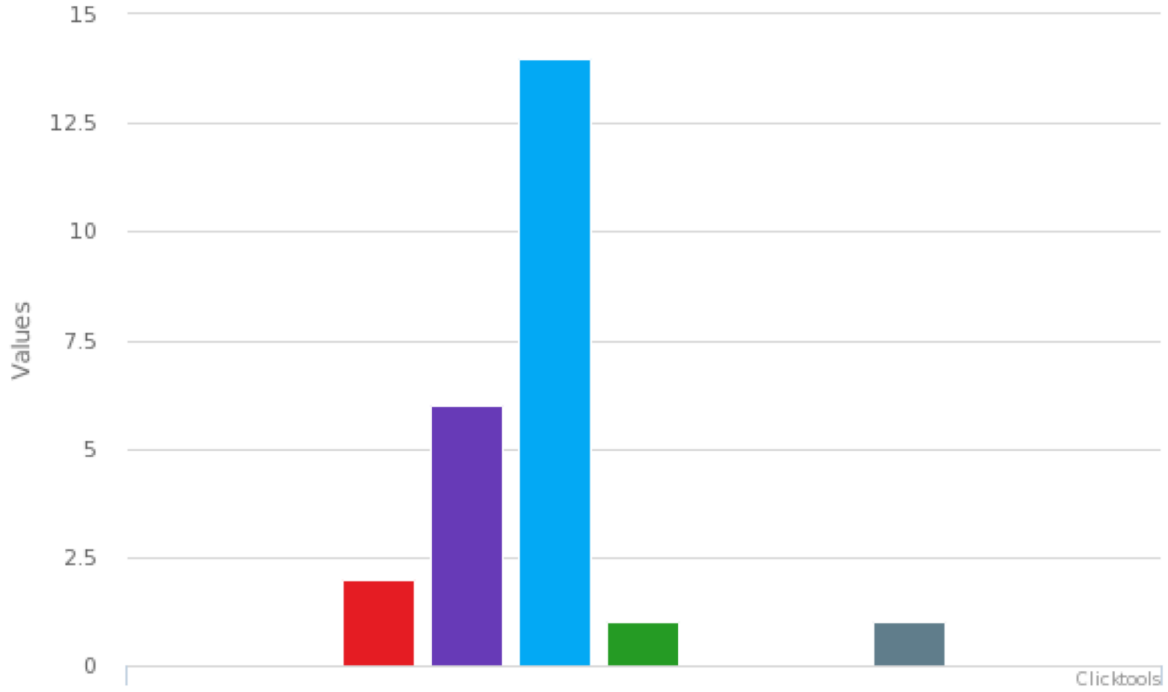



Clicktools

| | | | |
|---|---|---|---|
| 1 - Yes | 43.64% (24) | 2 - No | 47.27% (26) |
| 3 - I don't know | 9.09% (5) | | |

Mean: 1.65
Response: 55

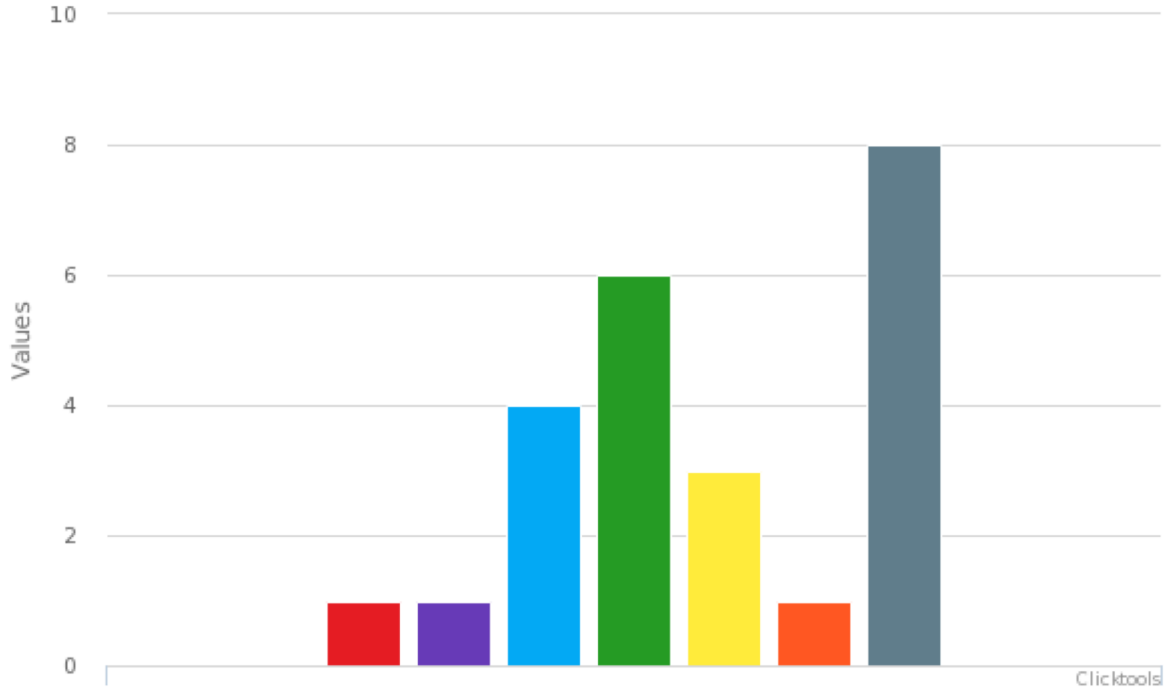
## 31. How many WHOIS lookups do you personally make per month as of June 2018?




| | | | |
|---|---|---|---|
| 1 - Same as before/no change | 8.33% (2) | 2 - <10 | 25% (6) |
| 3 - Between 10 and 100 | 58.33% (14) | 4 - Between 100 and 1000 | 4.17% (1) |
| 5 - Between 1000 and 10000 | 0% (0) | 6 - >10000 | 0% (0) |
| 7 - None | 4.17% (1) | | |

Response: 24

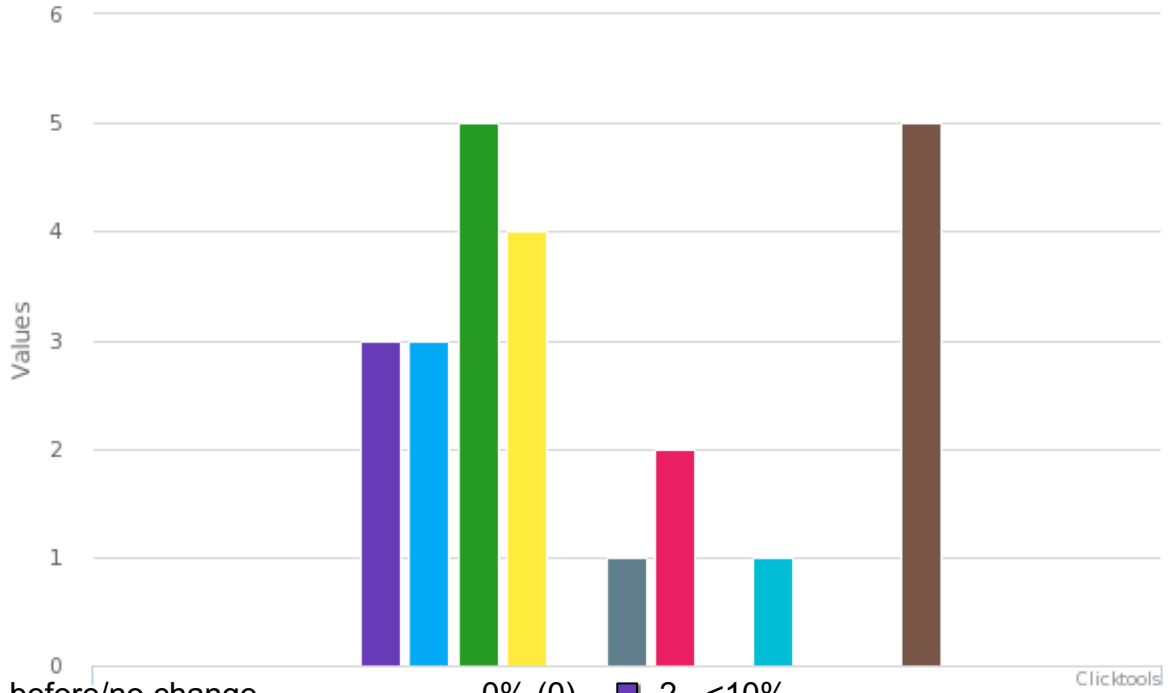
**32. How many lookups does your unit or other units or agencies in your jurisdiction whose use you are aware of make as of June 2018?**




| | | | |
|---|---|---|---|
| 1 - Same as before/no change | 4.17% (1) | 2 - <10 | 4.17% (1) |
| 3 - between 10 and 100 | 16.67% (4) | 4 - between 100 and 1000 | 25% (6) |
| 5 - between 1000 and 10000 | 12.5% (3) | 6 - >10000 | 4.17% (1) |
| 7 - I don't know | 33.33% (8) | | |

Response: 24

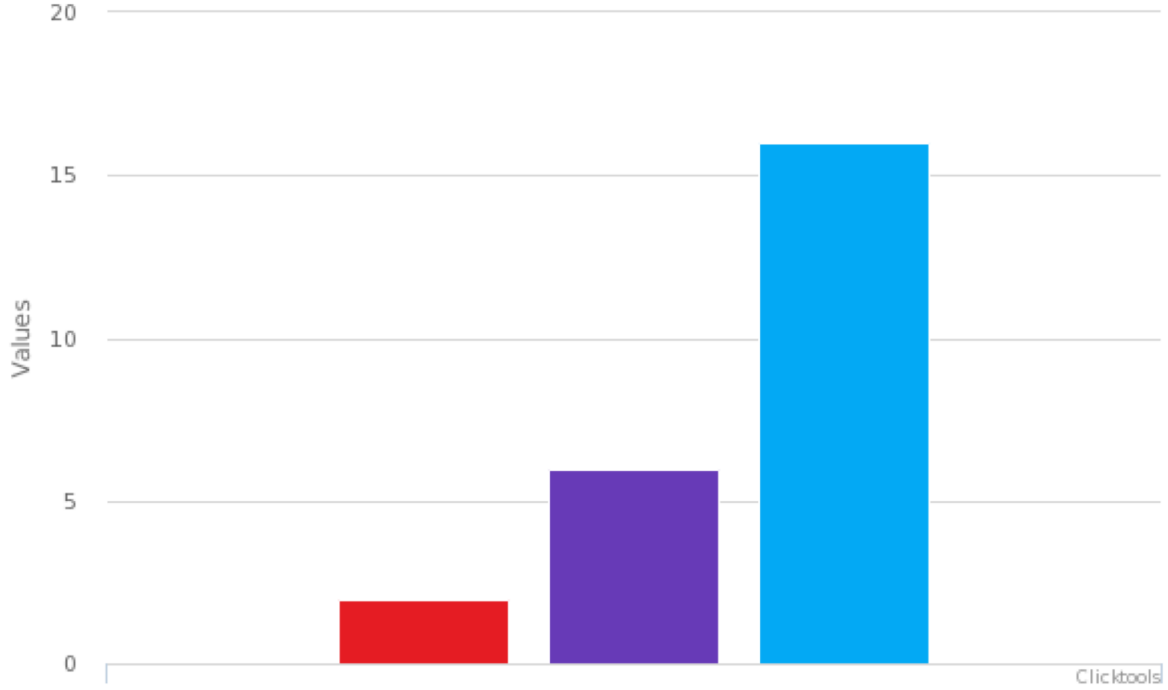
**33. Generally speaking, what is the percentage of WHOIS lookup results that help your investigation?**




| | | | |
|---|---|---|---|
| 1 - Same as before/no change | 0% (0) | 2 - <10% | 12.5% (3) |
| 3 - 10% | 12.5% (3) | 4 - 20% | 20.83% (5) |
| 5 - 30% | 16.67% (4) | 6 - 40% | 0% (0) |
| 7 - 50% | 4.17% (1) | 8 - 60% | 8.33% (2) |
| 9 - 70% | 0% (0) | 10 - 80% | 4.17% (1) |
| 11 - 90% | 0% (0) | 12 - 100% | 0% (0) |
| 13 - I don't know | 20.83% (5) | | |

Response: 24

**34. Does the current WHOIS lookup functionality (personal data, e.g. name, email address, phone number, postal address being redacted by some registrars) meet your needs for the purposes of law enforcement investigations?**




| | | | |
|---|---|---|---|
| 1 - Yes | 8.33% (2) | 2 - Partially | 25% (6) |
| 3 - No | 66.67% (16) | | |

Response: 24

## 35. How does it not meet your needs?


Clicktools

| | | | |
|---|---|---|---|
| 1 - Lack of personal data hinders the attribution of malicious domains | 90.91% (20) | 2 - Inaccurate data | 0% (0) |
| 3 - Other | 9.09% (2) | | |

Mean: 1.18
Response: 22

**36. Please specify in what way the WHOIS does not meet your needs.**
**Please specify whether your answer refers to your unit or also includes other units or agencies.**

| | |
|---|---|
| 1 | Generally, whois data was used for preliminary investigation to quickly identify possible registrant details and jurisdiction where it is being hosted. However with the redated information, it cause the preliminary investigation not about to proceed |
| 2 | Non-unifrom approach across all parties, Non timely access, Loss of confidentiality of request |
| 3 | The main function of WHOIS data is for cross-referencing and finding patterns between different domains. Given that there is essentially no information available it is hard to cross-reference and actually use the information to move forward. |
| 4 | Critical data is redacted |
| 5 | There is not possible to send 1000 request a month to different registrars and wait for the result who sometimes doesn`t come. |
| 6 | We (as agency) need more data even to identify owners or to work with incidents related to specific domain (e.g. verified owner), anonymity here is very bad for us |
| 7 | Inavailability of the data |
| 8 | There is no possible to contact the responsible person |
| 9 | answers only for me |
| 10 | see answer to question 35. |
| 11 | Lack of personal information |
| 12 | Lack of data + inconsitent and slow procedures - Unit |

**36. Please specify in what way the WHOIS does not meet your needs.**
**Please specify whether your answer refers to your unit or also includes other units or agencies.**

| | |
|---|---|
| 13 | In the past, a whois query could quickly confirm or eliminate the need for further investigative follow up (legal request, search warrant). The speed with which this happens can be as useful as access to more detailed records. |
| 14 | The criminal investigations on the internet are severely disrupted. There is no more an easy way to find out who is behind a domain that is being used to commit a crime. This is a real threat to a public safety. |
| 15 | On the basis of the same WHOIS information, it's possible for us to find out the related malicious domains.If the related information is masked, this method will not work.My answer refers to my unit. |
| 16 | In most of cases the information is either GDPR masked or hidden by privacy / proxy service providers. Answer is on behalf of our own unit, but I assume that others also agree |
| 17 | Lack of information can delay the investigation. Answer refers to Finnish Police. |
| 18 | For my Agency registrant full info is extremely useful, invaluable and conducive to our investigations. Lack of such data hinders our effectiveness and further investigation is considered extremely difficult or impossible. |
| 19 | MY UNIT - POOR QUALITY AND LOW INFORMATION |
| 20 | --- |
| 21 | Not only maliccious domains but to leads to converting into possible real world identity. |

## 37. Are there any other comments you would like to share with the review team should be aware of?

| | |
|---|---|
| 1 | maybe some sort of specific portal for registered law enforcement officers or agencies will be more helpful with much more abundant data, both present and previous records. |
| 2 | The relevance of whois to law enforcement investigation all over the world is critical as such that privacy laws should not be seen as providing a shield |
| 3 | In one way another, LEA do relay very much on WHOIS data for preliminary investigation even though the data will not be used during prosecution. It is still essential for LEA to be accessible to these data so that they know where and who they can approach |
| 4 | The impact is currently not being fully felt due to the availability of historic data, however once this data becomes too old more impact will be felt. |
| 5 | For question 35 - we would rather argue, that very often the whois data is inaccurate, but it still gives you some information, because the "inaccurate data" is reused by criminals. |
| 6 | 16 & 26 should have detailed the mechanism to determine that information accurately should have been provided to answer fully |
| 7 | there is need to open up the WHOIS Database as it was pre May 2018 |
| 8 | For Scam Site and Spear Mail investigation case, lack of registrant's name and real estate address on WHOIS data is lethally negative impact. |
| 9 | In my searches I found many fake registrant data, using the name of famous characters of shows, like "Tyrion Lannister" (Game of Thrones). |
| 10 | There is a need for a very quick solution for accreditation. The only winner of GDPR is those of the dark side of the net. Otherwise it will be huge problems with the infrastructure of the Internet. |

## 37. Are there any other comments you would like to share with the review team should be aware of?

| | |
|---|---|
| 11 | Also data from other regions needed (Africa, Azia...) |
| 12 | WHOIS data is very important in law enforcement and its unavailability advantages cybercriminals |
| 13 | During the investigation the on-line access to required data is necessary. |
| 14 | While usage has not changed, the impact of reduced results has increased and impeded investigations. The correct balance between protecting citizens and protecting privacy has not been reached. |
| 15 | By masking the registrant in WHOIS will impede investigation and make solving crimes more and more difficult. |
| 16 | no |
| 17 | who is service is a very important part of investigation against cybercrime and cyber attacks thus police agencies needs full access to whois and look up services and without this accees they will not be able to investigate any cases. |
| 18 | From a law enforcement perspective information, that often is "faked" is being protected.If there is a need of gated access there should only be ONE central authority(ICANN) for this(access authorization, data acquisition).No more due to FIELD LIMITATION! |
| 19 | Even if we do not yet experience significant problems, the actual changes to the WHOIS lookup need to be addressed so LE can still have access to the information needed for investigative purposes!!! |
| 20 | Official LE requests to obtain detailed WHOIS records (info that was publicly available prior to May 2018) is time consuming and potential unnecessary, as this information could eliminate certain domains from further scrutiny. |

## 37. Are there any other comments you would like to share with the review team should be aware of?

| | |
|---|---|
| 21 | N/A |
| 22 | We hope that there will be a way for LEAs to obtain the WHOIS information for detection and prevention of crime. |
| 23 | We are prone to be submitted to vetting or other necessary controls to access this privileged data, but in contrast the database should include quality information validated for the registrar or other mechanisms that may assure real registrant information |
| 24 | My experience is more about Asia.So we have little influence by the GDPR in comparison to EU LE.I believe. |
| 25 | No, thanks |
| 26 | N/A |
| 27 | Exempt Law enforcement Agencies. |
| 28 | No |
| 29 | Things change rapidly and constantly. LEAs should be more regularly asked for these kind of surveys. Their opinion matter, on the grounds that they mostly encounter malicious online activities which sometimes individuals are not aware of. |
| 30 | now we can´t see persona data name, email, phone and other information, how can we access to that? |
| 31 | The redaction of PII data does not only imapct within the intelligence of domains. This in my experience is often the seed data in other databases beyond the scope of domain data. Loosing the visibility of seed data it impacts the intelligence collection |