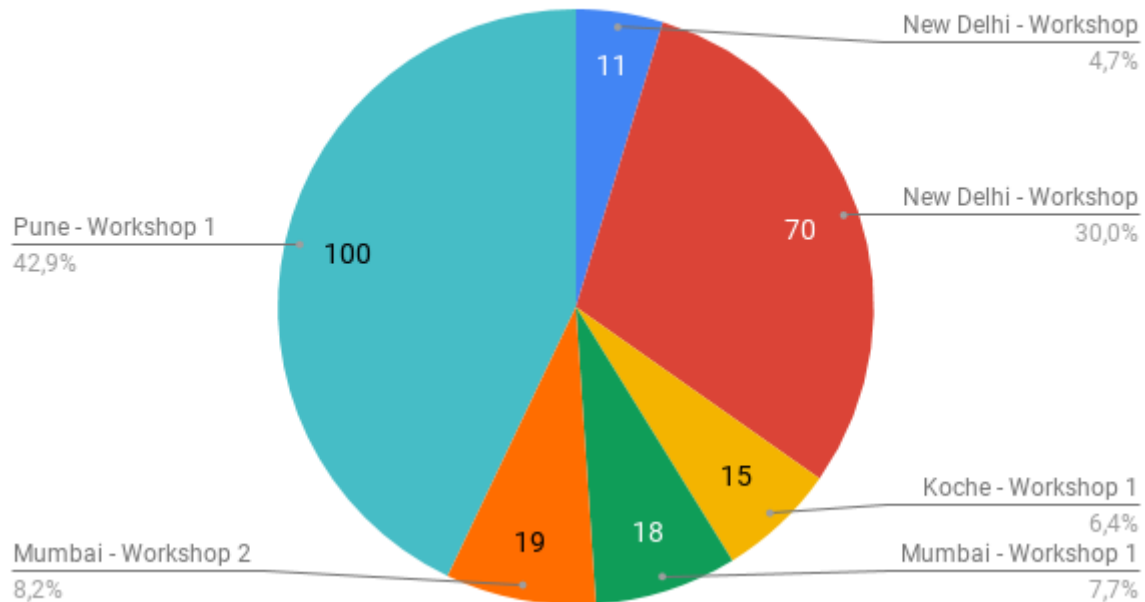


Table of Contents

Demographics.....	2
Interviews.....	2
Activities.....	5
New Delhi.....	5
#1 Workshop.....	5
#2 Workshop.....	6
Koche.....	7
#1 Workshop.....	7
Mumbai.....	7
#1 Workshop.....	7
#2 Workshop.....	9
Pune.....	11
#1 Workshop.....	11
Interview Quotes.....	12

Demographics

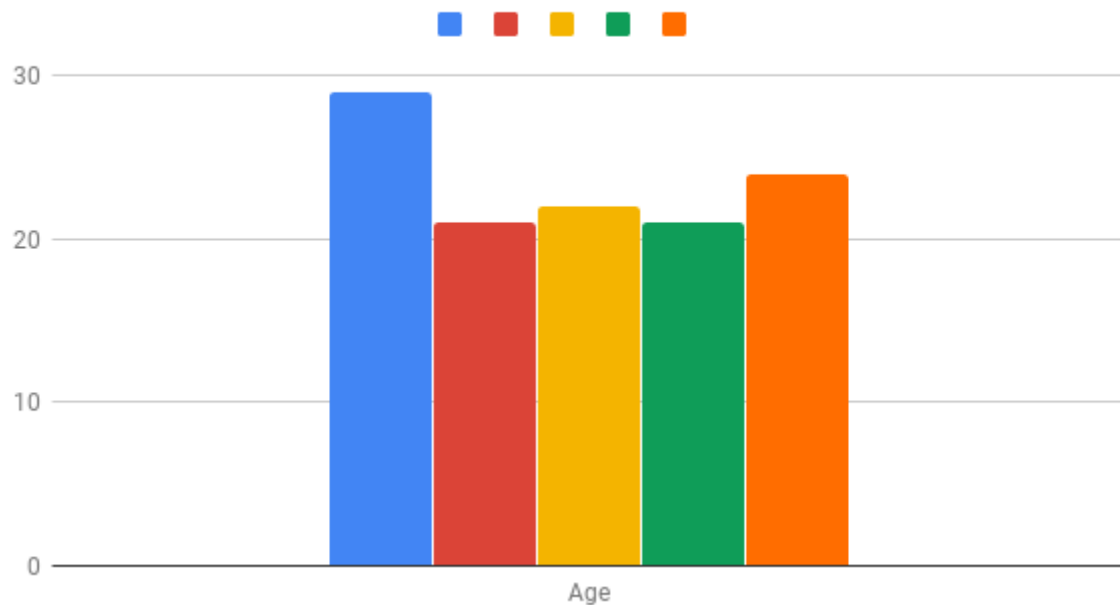
Total Reach: ~233



Note: Most of the audience were students, the number with more audience represents public events.

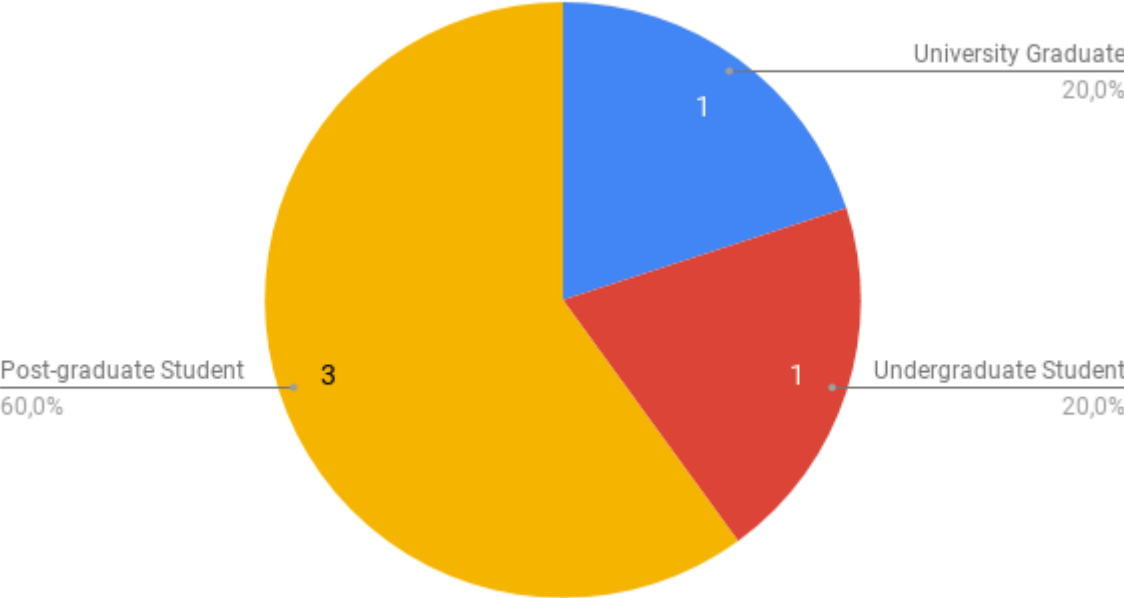
Interviews

How old are you?

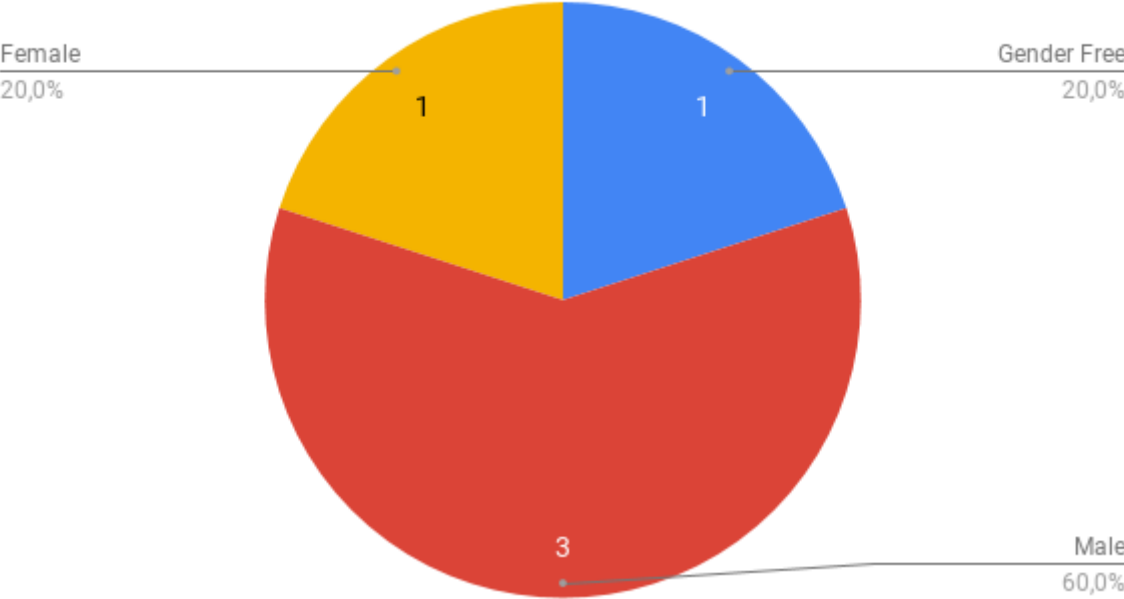


Note: All interviewees were young, i.e. under 30 years old.

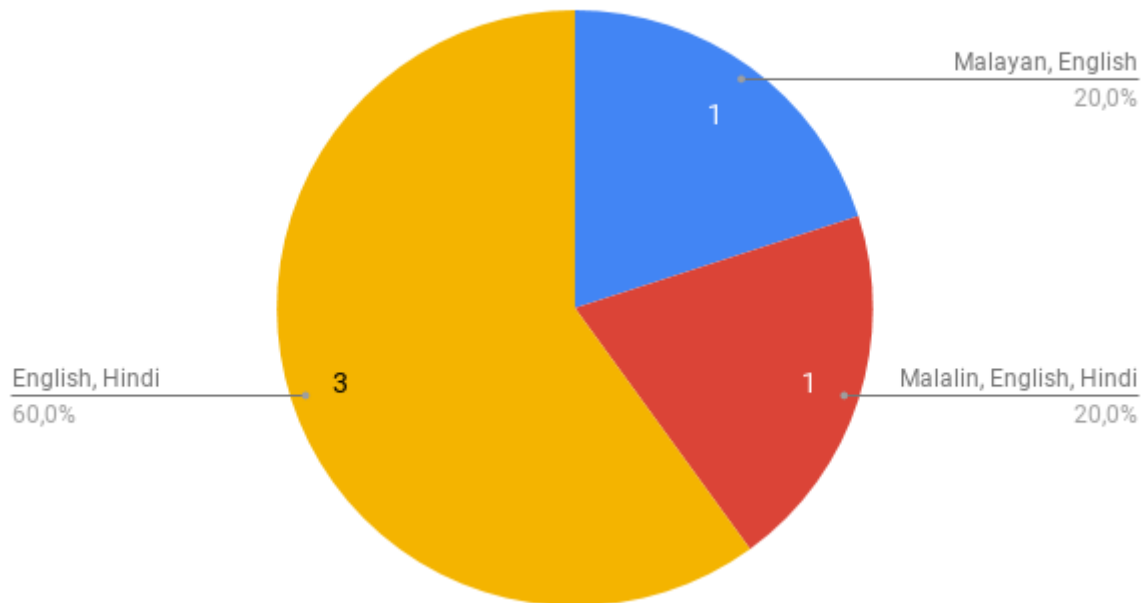
Education Level



Gender

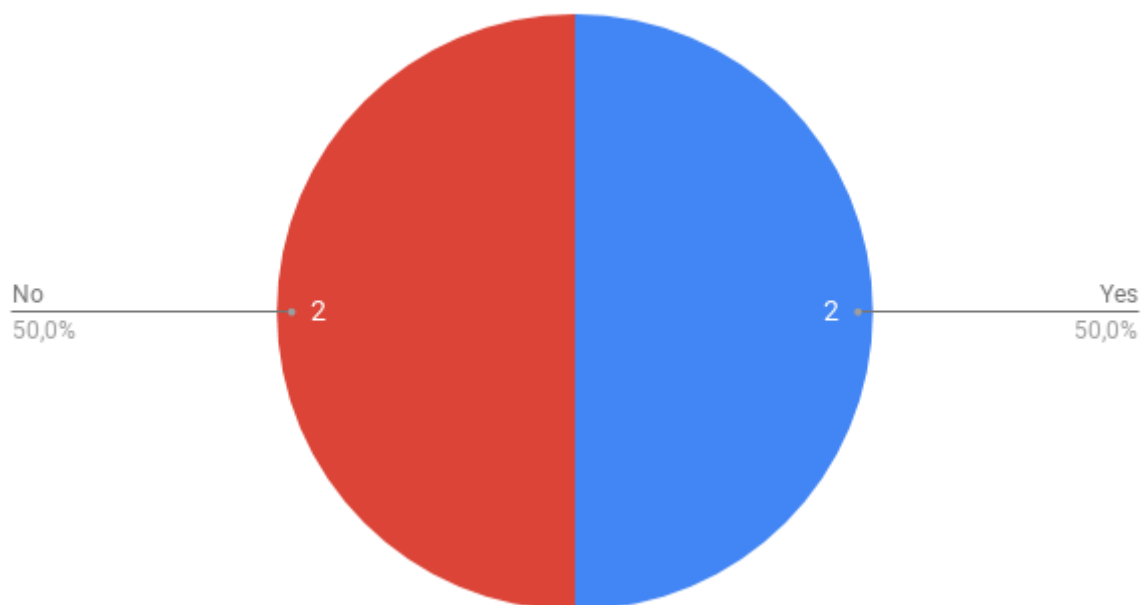


Languages Spoken



Note: All interviewees are currently living in India; only one of the interviewees identifies themselves as minority. Two out of five of the interviewees doesn't have a religion.

Have you used Tor before? If so, how often?



Note: from those who use Tor Browser, they used for different reasons (not specified). Everyone of them use other browsers too.

Activities

Workshops

- 2 Workshops in New Delhi:
 - Tor training and Threat Model;
 - Tor training and User Needs Discovery.
- 1 Workshop in Koche;
- 2 Workshops in Mumbai:
 - Tor presentation;
 - Digital Security Training with Threat Model.
- 1 Workshop in Pune:
 - Digital Security Training and User Testing

Interviews:

- 1 demographics's from Koche.
- 6 Interviews made are registered.

New Delhi

#1 Workshop

When: February 12th

Audience: journalists, lawyers, technologists.

People: 11

Agenda:

Tor Training

Threat model exercise

Threat Model

Assets	
Mails from publishers and sources	Private communication with clients

Threats	
Government	Political and personal adversaries

Questions

- The tools I can use along with Tor to make my assets secure? (mail clients, etc.)
- What about my communication from other mobile apps?
- Does using Tor with VPN make it more secure for me?
- Can I hide the fact that I am using Tor? (most participants were unaware of bridges and pluggable transports)

Suggestions from the audience

- Including a course or module on cyber security in the journalism and law curriculums in the country
- **Organising Tor sessions on campuses of prominent journalism and law institutes in the country to train professionals early on.**
- A general interest in participating in #tor-south meetings. (Community)

#2 Workshop

When: February 12th

Audience: Students (from freshman to final year, mainly computer science grads but other streams also present).

People: 60-70.

Agenda:

Tor Training

User needs discovery

Findings and Observation:

- Most users did not face any problems with any of the tasks, owing to their comfort levels in using the internet.

- During general interaction, most users reported finding the on-boarding experience friendly and helpful, some had problems with accessing the .onion link.
- A lot of students were interested in knowing about the deep and dark web.
- Some students were interested in contributing to Tor.

Koche

#1 Workshop

When: February 18th

Audience: Male

People: 15

Title: Tor Project: Internet Security and Privacy Online

Context:

Some students (first year students of computing), web developer, new relay operator, debian developer, IT crowd in general.

About 5 people had heard of Tor before others had an interest in it.

Mumbai

#1 Workshop

Title: Tor presentation

When: February 22nd

Audience: About 5 FOSSE folks.

People: twenty, 18 men, 02 women,

Context: very interested audience, some of the were from startups and companies. There were also a digital policy fellow.

Quotes:

- **"I don't really think I need privacy** so I want to understand more"
- "I have heard about Tor before and the Silk Road and I want to learn more about the dark web"
- "How is this different from what a VPN does?"
- "Alexandra (scihub) is doing the same that Aaron Schwartz was doing"

Questions:

- "Is tor a P2P network?"
- "Can I use the tor network to browse normal https websites?"
- "What is the country of origin for a request from the tor network?" (When visiting a website)
- "Is the client aware of each encryption key it needs to use to send data on the network and the path that it is going to take on the network?"
- "Is it possible to find out the path that a client is taking on the Tor Network?"
- "What about the attacks that have happened with blockchain" - Sybill attacks
- "Can you change the Tor circuit every time?"
- "If you log into facebook, facebook knows everything about you?"
- "Who makes the DNS request when using the Tor network?"
- "Is there any sort of DNS caching on the exit node?"
- "If my exit node is in germany will I see the german google version?"
- "How is the browsing experience different using Tor Browser?"
- "Is it possible to have more than 1 middle node?"
- "Where is the directory of relays maintained?"
- "Why doesn't the ISP just block Tor?"
- "Does Tor work in China?"
- "For IOT related applications, can I use other protocols other than HTTP with Tor?"
- "What happens when a new exit node is created, is Netflix going to know about it to block it?"
- "Was Aaron Schwartz using the Tor Network?"
- "Why are the fonts disabled in the safer security level?"
- "Is there any way to connect to irc through Tor?"
- "Can you use i2p with Tor?"
- "Is it trackable if someone commits a crime using my exit node?"
- "How does the Tor Project avoid "prosecution" from governments given that we allow censorship circumvention?"
- "Why does the Tor Project not work with governments more to ensure its continued existence?"
- "How can I change my circuit if I'm not using Tor Browser?"
- "What is the deepweb?"

- "How difficult is it for me to reverse the 3 hops?" / "How to de-anonymise a user on the Tor network?"
- "Why does facebook have an onion site yet at the same time is working with the CHinese gvt to allow facebook in the country?"
- "Is everything going through the Tor Browser?" (OnionShare)
- "Do both computers need to be on in order to send and receive?" (OnionShare)
- "How is the Tor project sustained?" (Funding)

#2 Workshop

Title: Digital Security Training

When: February 22nd.

People: 19 people / 9 men, 9 women

Context:

- one person had used tor browser before
- Some people kept coming and going

Agenda:

Threat Modelling

Using Password Manager

Signal

Quotes

- **"If it's open source you can hack it"** – Signal
- **Bill Gates would be very sympathetic to your cause**

Other comments

- Lots of questions about password management
- Lots of questions about sim card cloning
- Sometimes you need to access websites but they are blocked and the only way to access is a VPN

Questions:

- "Do I need to use 2FA to log into my computer every time?"
- "Isn't it enough to have a really long password?"

- "What about using a database to store password?"
- "How are password managers different from spreadsheets or databases?"
- "How different is this from the incognito mode in chrome?"
- "Do we need to use VPN along with Tor"
- "Can you use Tor for money transfers? What about cryptocurrencies?"
- "If the police came to arrest me, How much of my information can Tor give them about my usage?"
- "How many current users of Tor in India atm?"

Signal

- "What is the difference between Telegram and Signal?"
- "Whatsapp asks for lots of permission? Does signal also asks for those permissions?"

Tor Browser

- "Why is it nearly nothing?" (When talking about tor browser writing to disk)
- "If we're using Tor Browser we won't get the options we get when we've searched the same term?"
- "How does Tor Browser block fingerprinting?"
- "How does greater use of AI impact thsi?"
- "Why does Tor Browser ask me (not?) to change my screen size?"
- "How is Tor Browser for Android better than Orfox"
- "There are people in China who access people through Tor?"
- "Is Tor Browser based on Firefox?"

OnionShare

- "How does the data transmission happen if you don't upload the file anywhere?"

Funding

- "When things are free like Tor, how do you make money?"

Pune

#1 Workshop

When: February 20th

Audience: Students

People: About 100 students

Agenda:

Tor Presentation

Digital Security Training (Kushal)

User Testing

Quotes:

- “Tor Browser is an Open Source Browser from Mozilla”
- **"Even though we have encryption on the relays, it can still be decrypted by the relay"**
- "Trusting Tor is like trusting these 11 relay authorities"
- "Google will know what you are searching for even if you use Tor Browser with it"

Other:

- About half of students have Tor installed already
- Good understanding of incognito mode in chrome and other browsers

Questions:

- Is there any way to track someone that is using Tor Browser back to its node?
- What is the probability that some relays are not malicious?
- **Why can't Tor steal our data?**
- What is stopping an intelligence agency from hosting these relays? Both entry and exit nodes for time based attacks? How does Tor prevent that?
- Who are/run the directory authorities?
- Can I use the tor network for torrenting?
- Is it possible for governments to block Tor?

Tor Browser:

- Can the Tor network support all protocols?

OnionShare:

- If OnionShare is free are you not the product?
- Why does onion share have a http address? Should it not have a https address?
- The .onion address, that must be the address of my machine?
- How is OnionShare different from WeTransfer?

OnionService:

- How do you deal with impersonation of onion service addresses?
- Are the same set of relays used for communication between a hidden service and a client? What about when multiple requests are made?

Funding:

- Who donates to Tor? Is it just individuals? What kind of people donate to Tor?

Interview Quotes

Although it seems to be intuitive to go to the shield and change the Security Settings, most users come to a block, from the interviews we could understand there was a bug with the Security Settings.

Interviewee 2: *"I think I prefer the old demo. the onion was better. it was more intuitive."*

Interviewee 4 wasn't able to navigate.

Interviewee 5:

Question: Why did we decide to go with a Shield to change the security settings instead on keeping it on the Setting/Preferences menu as other browsers?