A dark blue, irregular ink blot or watercolor splash serves as a background for the text. The blot has a textured, slightly grainy appearance with some lighter blue and white areas around its edges, suggesting a liquid or painted effect. The text is centered within the blot in a clean, white, sans-serif font.

Практическая работа №7

Upload Bandwidth

Freq Band Indicator7

Download Frequency

Num Tx Antennas

UARFCN3457

Tracking Area Code27050

Cell Identity19875


Physical Cell ID1

Upload Frequency

Download Bandwidth

1. Определение
идентификаторов
базовой станции

Местонахождение базовых станций

МСС: ручной ввод: выбор: 250 Россия 
Mobile Country Code (код страны)

MNC:
ручной ввод: выбор: Теле-2, АКС ▾
Mobile Network Code (код сети)

LAC / TAC:
dec: hex:
2 16

Location Area Code (код местности).
Вводите в десятичном (dec) или
шестнадцатеричном (hex) формате

CID / SAC / ECI:
dec: 190 hex: bc

Cell ID (идентификатор соты).
Вводите в десятичном (dec) или шестнадцатеричном (hex) формате

получить местонахождение



[x] отображать зону действия базовых станций

Радиус зоны действия в метрах: 350

Усредненное значение:

координаты.

2. Отображение на карте

```
Файл Действия Правка Вид Справка
enon@kali:~$ sudo arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:4e:b6:22, IPv4: 192.168.1.82
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.70 [REDACTED] AzureWave Technology Inc.
192.168.1.72 [REDACTED] MITAC INTERNATIONAL CORP.
192.168.1.72 [REDACTED] MITAC INTERNATIONAL CORP. (DUP: 2)
192.168.1.73 [REDACTED] GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.73 [REDACTED] GIGA-BYTE TECHNOLOGY CO.,LTD. (DUP: 2)
192.168.1.74 [REDACTED] Hon Hai Precision Ind. Co.,Ltd.
192.168.1.75 [REDACTED] GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.75 [REDACTED] GIGA-BYTE TECHNOLOGY CO.,LTD. (DUP: 2)
192.168.1.254 [REDACTED] DWnet Technologies(Suzhou) Corporation
192.168.1.254 [REDACTED] DWnet Technologies(Suzhou) Corporation (DUP: 2)

10 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.810 seconds (91.10 hosts/sec). 10 responded
enon@kali:~$ macchanger -s eth0
Current MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
enon@kali:~$ macchanger -A eth0
Current MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
[ERROR] Could not change MAC: interface up or insufficient permissions: Operation not permitted
enon@kali:~$ sudo macchanger -A eth0
Current MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:4e:b6:22 (CADMUS COMPUTER SYSTEMS)
New MAC: 6c:b3:50:9e:a0:60 (Anhui comhigher tech co.,ltd)
enon@kali:~$
```

3. Смена MAC адреса


```
Файл Действия Правка Вид Справка
enon@kali: ~
enon@kali:~$ curl ipinfo.io
{
  "ip": "109.252.125.37",
  "hostname": "109-252-125-37.nat.spd-mgts.ru",
  "city": "Moscow",
  "region": "Moscow",
  "country": "RU",
  "loc": "55.7522,37.6156",
  "org": "AS25513 PJSC Moscow city telephone network",
  "postal": "101000",
  "timezone": "Europe/Moscow",
  "readme": "https://ipinfo.io/missingauth"
}
enon@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:4e:b6:22 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.82/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 86193sec preferred_lft 86193sec
   inet6 fe80::a00:27ff:fe4e:b622/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
enon@kali:~$
```

4. Сравнение WAN и LAN

Файл Действия Правка Вид Справка

```
enon@kali:~$ proxychains curl ipinfo.io
ProxyChains-3.1 (http://proxychains.sf.net)
DNS-request| ipinfo.io
S-chain|-72.221.164.34:60671-4.2.2.2:53-OK
DNS-response| ipinfo.io is 216.239.36.21
S-chain|-72.221.164.34:60671-216.239.36.21:80-OK
{
  "ip": "72.221.164.34",
  "city": "Atlantic City",
  "region": "New Jersey",
  "country": "US",
  "loc": "39.3642,-74.4231",
  "org": "AS22773 Cox Communications Inc.",
  "postal": "08404",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
```

Браузер

Загрузки

Сеть

Десктоп

kali@kali:~\$

Браузер

Загрузки

Сеть

Десктоп

5. Использование прокси

```

Настраивается пакет tor (0.4.4.6-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Настраивается пакет torsocks (2.3.0-3) ...
Настраивается пакет tor-geoipdb (0.4.4.6-1) ...
Обрабатываются триггеры для systemd (245.6-2) ...
Обрабатываются триггеры для man-db (2.9.3-2) ...
Обрабатываются триггеры для kali-menu (2020.3.2) ...
enon@kali:~$ sudo systemctl enable tor
Synchronizing state of tor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable tor
Created symlink /etc/systemd/system/multi-user.target.wants/tor.service → /lib/systemd/system/tor.service.
enon@kali:~$ sudo systemctl start tor
enon@kali:~$ curl ipinfo.io
{
  "ip": "109.252.125.37",
  "hostname": "109-252-125-37.nat.spd-mgts.ru",
  "city": "Moscow",
  "region": "Moscow",
  "country": "RU",
  "loc": "55.7522,37.6156",
  "org": "AS25513 PJSC Moscow city telephone network",
  "postal": "101000",
  "timezone": "Europe/Moscow",
  "readme": "https://ipinfo.io/missingauth"
}
enon@kali:~$ curl --socks5 127.1:9050 -L ipinfo.io
{
  "ip": "77.247.181.162",
  "hostname": "chomsky.torserver.net",
  "city": "Soest",
  "region": "Utrecht",
  "country": "NL",
  "loc": "52.1733,5.2917",
  "org": "AS43350 NForce Entertainment B.V.",
  "postal": "3765",
  "timezone": "Europe/Amsterdam",
  "readme": "https://ipinfo.io/missingauth"
}
enon@kali:~$ python3 -m http.server --bind 127.0.0.1 8080
Serving HTTP on 127.0.0.1 port 8080 (http://127.0.0.1:8080/) ...
127.0.0.1 - - [11/Dec/2020 02:01:55] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [11/Dec/2020 02:01:55] code 404, message File not found
127.0.0.1 - - [11/Dec/2020 02:01:55] "GET /favicon.ico HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.
enon@kali:~$ whereis tor
tor: /usr/bin/tor /usr/sbin/tor /etc/tor /usr/share/tor /usr/share/man/man1/tor.1.gz
enon@kali:~$ sudo nano /etc/tor/torrc
enon@kali:~$ systemctl restart tor
enon@kali:~$ curl --socks5 127.1:9050 -L ipecho.net/plain
185.220.101.202
enon@kali:~$ █

```

6. Проверка работоспособности


```
enon@kali: ~  
Файл Действия Правка Вид Справка  
enon@kali:~$ sudo systemctl enable tor  
[sudo] пароль для enon:  
Попробуйте ещё раз.  
[sudo] пароль для enon:  
Synchronizing state of tor.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable tor  
Created symlink /etc/systemd/system/multi-user.target.wants/tor.service → /lib/systemd/system/tor.service.  
enon@kali:~$ sudo systemctl start tor  
enon@kali:~$ curl --socks5 127.1:9050 -L ipinfo.io  
{  
  "ip": "185.220.101.19",  
  "city": "Berlin",  
  "region": "Berlin",  
  "country": "DE",  
  "loc": "52.5244,13.4105",  
  "org": "AS208294 Markus Koch",  
  "postal": "10178",  
  "timezone": "Europe/Berlin",  
  "readme": "https://ipinfo.io/missingauth"  
}  
enon@kali:~$ sudo nano /etc/tor/torrc  
enon@kali:~$ systemctl restart tor  
enon@kali:~$ curl --socks5 127.1:9050 -L ipecho.net/plain  
185.220.101.210enon@kali:~$ ^C  
enon@kali:~$ tor  
Dec 11 04:17:43.729 [notice] Tor 0.4.4.6 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1g, Zlib 1.2.1  
Dec 11 04:17:43.729 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproje  
Dec 11 04:17:43.729 [notice] Read configuration file "/etc/tor/torrc".  
Dec 11 04:17:43.733 [warn] Directory /var/lib/tor/hidden_service/ cannot be read: Permission denied  
Dec 11 04:17:43.733 [warn] Failed to parse/validate config: Failed to configure rendezvous options. See logs for  
Dec 11 04:17:43.733 [err] Reading config failed--see warnings above.  
enon@kali:~$ python3 -m http.server --bind 127.0.0.1 8080  
Serving HTTP on 127.0.0.1 port 8080 (http://127.0.0.1:8080/) ...  
127.0.0.1 - - [11/Dec/2020 04:19:34] "GET / HTTP/1.1" 200 -  
127.0.0.1 - - [11/Dec/2020 04:19:35] code 404, message File not found  
127.0.0.1 - - [11/Dec/2020 04:19:35] "GET /favicon.ico HTTP/1.1" 404 -
```

Directory listing for /

2uircf3iovd06itduffpebvgsiqIs3ujn52myzi6ofk3oqc4snnkead.onion:8080

Directory listing for /

- [.bash_history](#)
- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)
- [.face](#)
- [.face.icon@](#)
- [.file.swp](#)
- [.gnupg/](#)
- [.ICEauthority](#)
- [.local/](#)
- [.mozilla/](#)
- [.pEp/](#)
- [.pEp_management.db](#)
- [.pEp_management.db-shm](#)
- [.pEp_management.db-wal](#)
- [.profile](#)
- [.ssh/](#)
- [.tf.swp](#)
- [.thunderbird/](#)
- [.yboxclient-clipboard.pid](#)
- [.yboxclient-display-svga-x11.pid](#)
- [.yboxclient-draganddrop.pid](#)
- [.yboxclient-seamless.pid](#)
- [.viminfo](#)
- [.Xauthority](#)
- [.xsession-errors](#)
- [.xsession-errors.old](#)
- [.zshrc](#)
- [daniel.neizvestno@gmail.com \(0xA99970DF3E6705A6687BB760D16A3B6BAE20BE7C\) rev.asc](#)
- [encrypted.asc](#)
- [fav11.gpg](#)
- [gpgkey.asc](#)
- [gpgkey1.asc](#)
- [gr](#)
- [group.sha1](#)
- [hid/](#)
- [Istinlih daniel.neizvestno@gmail.com \(0xD16A3B6BAE20BE7C\) pub.asc](#)
- [key.asc](#)
- [Notgroup.sha1](#)



8. Переход по
опион ссылке через
телефон

Файл Действия Правка Вид Справка

```
enon@kali:~$ torsocks ssh enon@jbsc2eswrcgkqv3gnb2lwsex35gn7f4fi6kcxnvnk4uyoinklyc3l4yd.onion -p20026 -i /home/enon/.ssh/id_rsa
```

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограни-

ок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

```
enon@kali:~$ smbclient //192.168.1.4/ -u Administrator -H 31d47c0:online
```

9. Подключение к ssh серверу по onion ссылке через аутентификацию по ключу

Консоль маршрутизатора I2P - Управление скрытыми сервисами - Mozilla Firefox

Консоль маршрутизатора I2P

Postman HQ » 1. Creating a ... | Postman HQ » 4. Account M... | OIB | Электронная почта - От ... | Электронная почта - Ло ...

127.0.0.1:7657/i2ptunnelmgr

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Версия: 0.9.48-0-1

Время Работы: 3 часа

Трафик (Вх./исх.)

3 С.: 0,12 / 1,21 KBps

5 Мин.: 0,21 / 1,07 KBps

Всего: 0,58 / 1,13 KBps

Объем: 6,47 MB / 12,32 MB

Сеть: Заблокирован брандмауэром

Службы I2P

Веб-сервер

Торренты

Эл. почта

Настройки I2P

Адресная книга

Графики

Журналы

Профили

Сетевая БД

Справка

Туннели

Узлы

Управление скрытыми сервисами

Справка И FAQ

Боковая панель

Доступность

История изменений

Решение проблем

Установка

ЧАВо

Юридическая информация

Узлы

Активные: 21 / 90

Быстрые: 24

Высокоемки: 52

Интегрированные: 344

Известные: 496

Туннели

Зондирующие: 6

Клиентские: 11

Транзитные: 0

Доля Транзита: 0,00

Принимаем туннели

PnC0ZyoMLc2Sb5pn~y1t~IZT1kF1XYdQ5arzCuR6~1j2i~nQGT17bGeLn7eMdUL4jX94p8liHIif2F79oBQAEAAcAAA==

Base32: npmb3op3v7msulau2ttacivbxvgrxa2ahverwrejmqqbigke4dxa.b32.i2p

Private key backup saved to /home/enon/.i2p/i2ptunnel-keyBackup/npmb3op3v7msulau2ttacivbxvgrxa2ahverwrejmqqbigke4dxa.b32.i2p-1607661576656.dat

Tunnels ready for client: Standard client on 127.0.0.1:7659

Client ready. listening on 127.0.0.1:7659

Глобальное управление туннелями

Мастер туннелей

Остановить все

Запустить все

Перезапустить все

Скрытые сервисы I2P

Название	Тип	Указывает на	Предпросмотр	Состояние	Управление
Die Gedanken sind frei	HTTP-сервер	127.0.0.1:8989	Предпросмотр	<div></div>	Остановить
Имя узла: agenda.i2p					
Описание: dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut					

Новый скрытый сервис: HTTP

Клиентские I2P-туннели

Название	Тип	Сетевой интерфейс	Порт	Состояние	Управление
I2P HTTP Proxy	HTTP/HTTPS клиент	127.0.0.1	4444	<div></div>	Остановить
Outproxy: false.i2p					
Общий клиент: HTTP proxy for browsing eepsites and the web					
Irc2P	IRC-клиент	127.0.0.1	6668	<div></div>	Остановить
Адрес назначения: irc.postman.i2p:6667,irc.echelon.i2p:6667					
Описание: IRC tunnel to access the Irc2P network					
pop3.postman.i2p	Обычный клиент	127.0.0.1	7660	<div></div>	Остановить
Адрес назначения: pop.postman.i2p:110					
Общий клиент: pop3 server					

10. Размещение сайта в I2P



11. Проверка работоспособности
скрытого сервиса через мобильный
клиент I2P