

ATENÇÃO AOS PROCEDIMENTOS DE SEGURANÇA

- Em casos de despressurização, chame o coleguinha ao lado ele deve chamar o pessoal de apoio do hotel.
- Nossa aeronave é equipada com detectores de Wifi, se tu subir um Ap Fake será identificado.
- Em caso de emergência luzes do piso e no teto acenderão automaticamente, mostrando 3 saídas de emergência localizadas no fundo da sala, se lascou quem sentou na frente ;)
- Em caso de falta de energia, ficaremos no escuro até o gerador ser acionado
- Por fim divirtam-se



MOTIVAÇÃO



"Last Call for SATCOM Security" escrito
pelo pesquisador Ruben Santamarta
(2018)

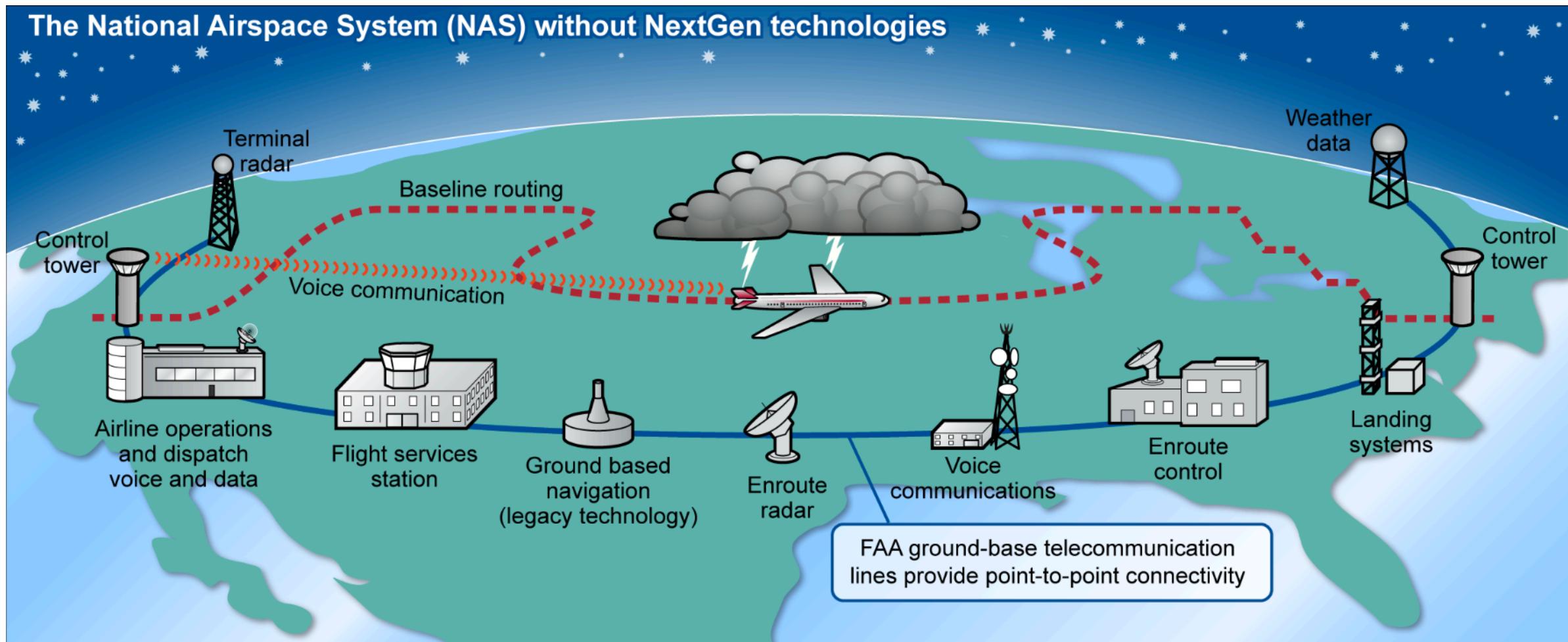


Wifi a bordo (Just for Fun!)

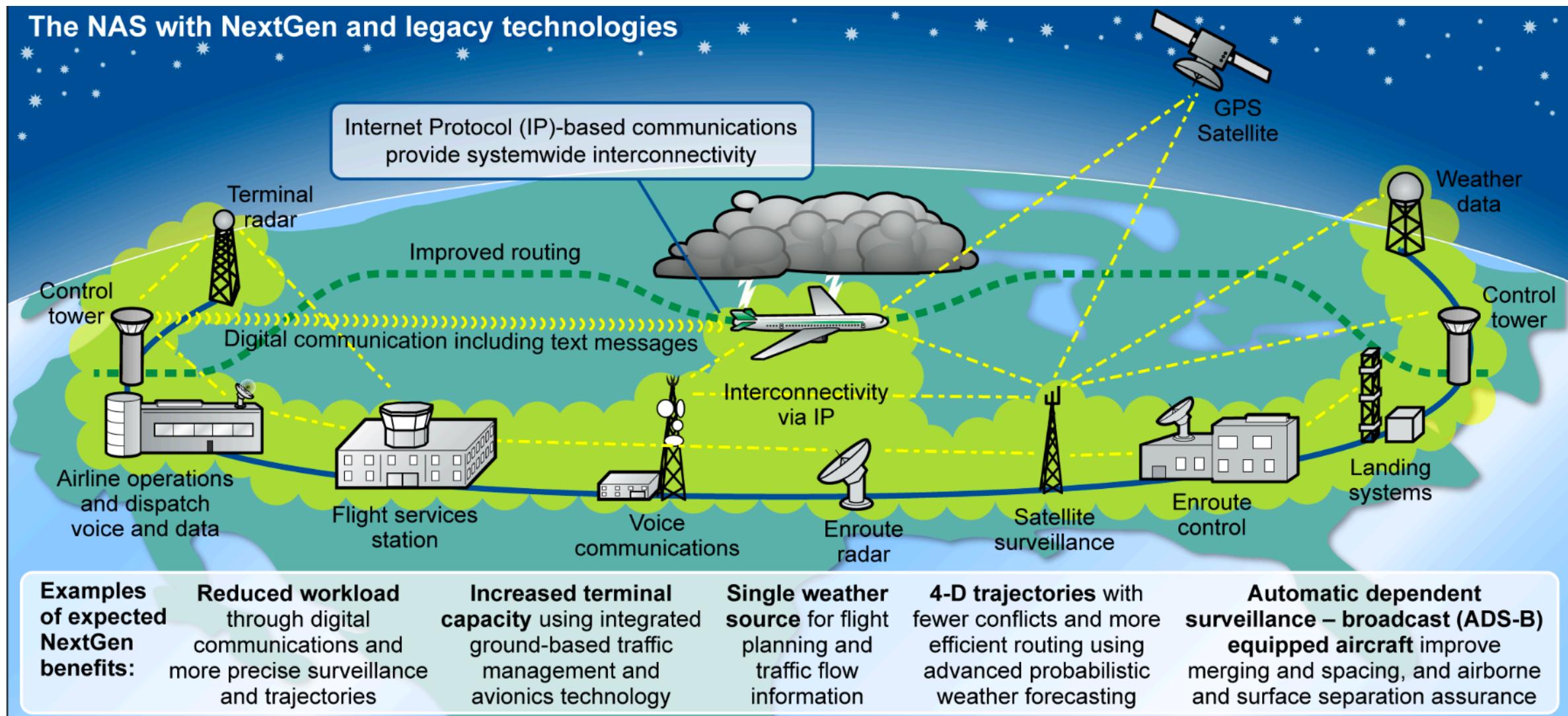


Desafio

ENTENDENDO UM POUCO O CENÁRIO



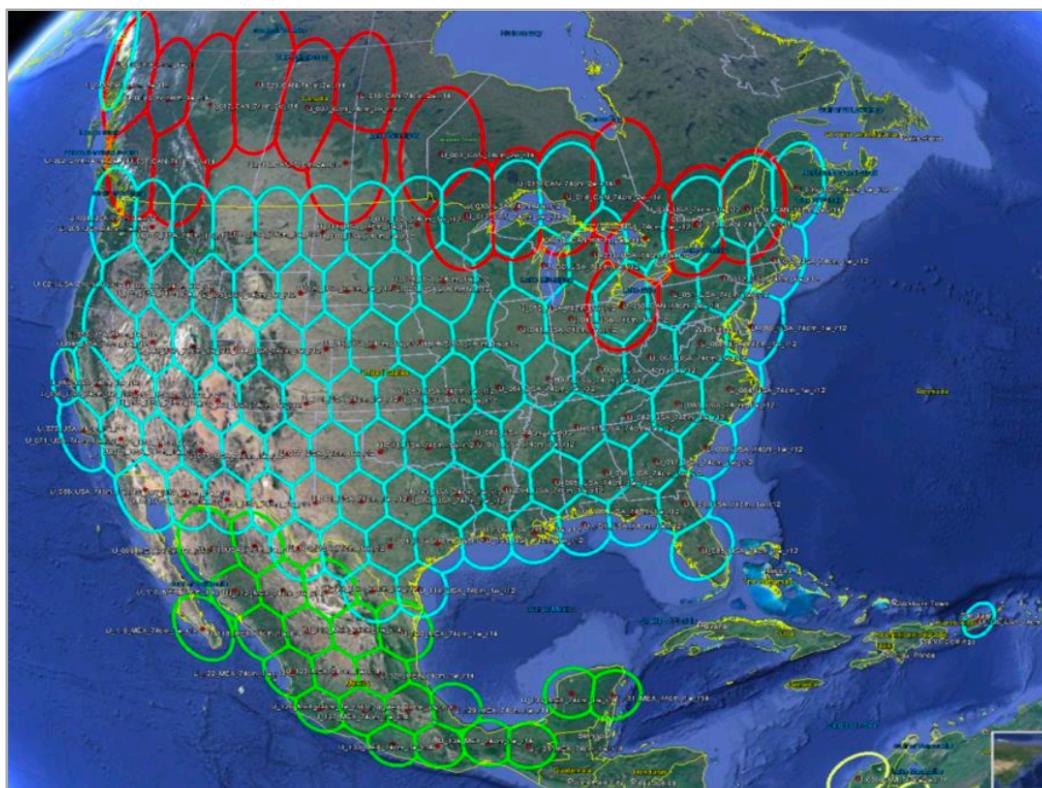
ENTENDENDO UM POUCO O CENÁRIO



RELEVÂNCIA DA PESQUISA

Start With Ka-Band GEO

Hughes Jupiter-1 and Jupiter-2
>300 Gbps total capacity



- 300 Gbps of available capacity, first priority access to bandwidth
- Spot beams for CONUS, Canada, Mexico, Central America, Caribbean
- 2.5 Gbps peak beam capacity
- Enhanced beam switching
- Future capacity on Jupiter-3 and SES-17 Ka-band satellites
- For 2018-2020, supplemental coverage and capacity from:
 - Telesat Anik Ka-band

OBJETIVOS



Diante dos diversos meios de conectividade contidos em uma aeronave, como é a segurança dos serviços de internet oferecido dentro das aeronaves?



Quais os ataques possíveis?

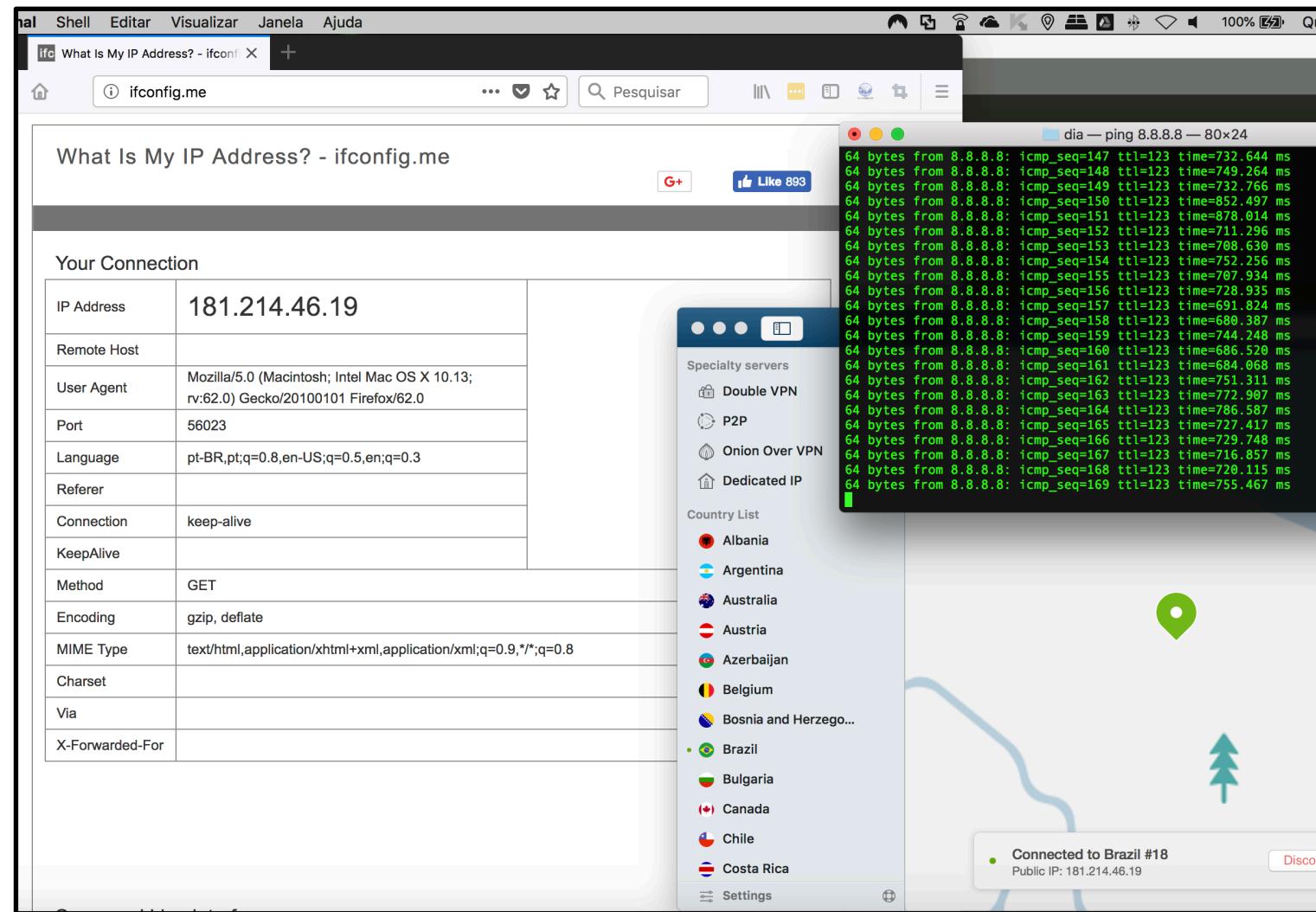


A pesquisa foi realizada em conjunto com uma companhia aérea com a intenção de identificar os riscos na prestação dos serviços aos tripulantes e a segurança da aeronave.

OBJETIVOS

Os testes foram realizados no serviço de acesso a internet na aeronave Airbus modelo: A320-214.

1. Seria possível utilizar a infraestrutura de wifi para realizar um ataque cibernético tendo como alvo outros equipamentos externo a infraestrutura da aeronave, ou seja equipamentos em solo?
2. Seria possível acessar equipamentos em solo através de acesso remoto tais como SSH e Remote Desktop?
3. Seria possível um visitante utilizar-se de contramedidas de privacidade afim de proteger os seus acessos e/ou utilizar-se deste subterfugio para ofuscar um ataque?
4. Seria possível de solo acessar e/ou comprometer um equipamento conectado no wifi da aeronave?



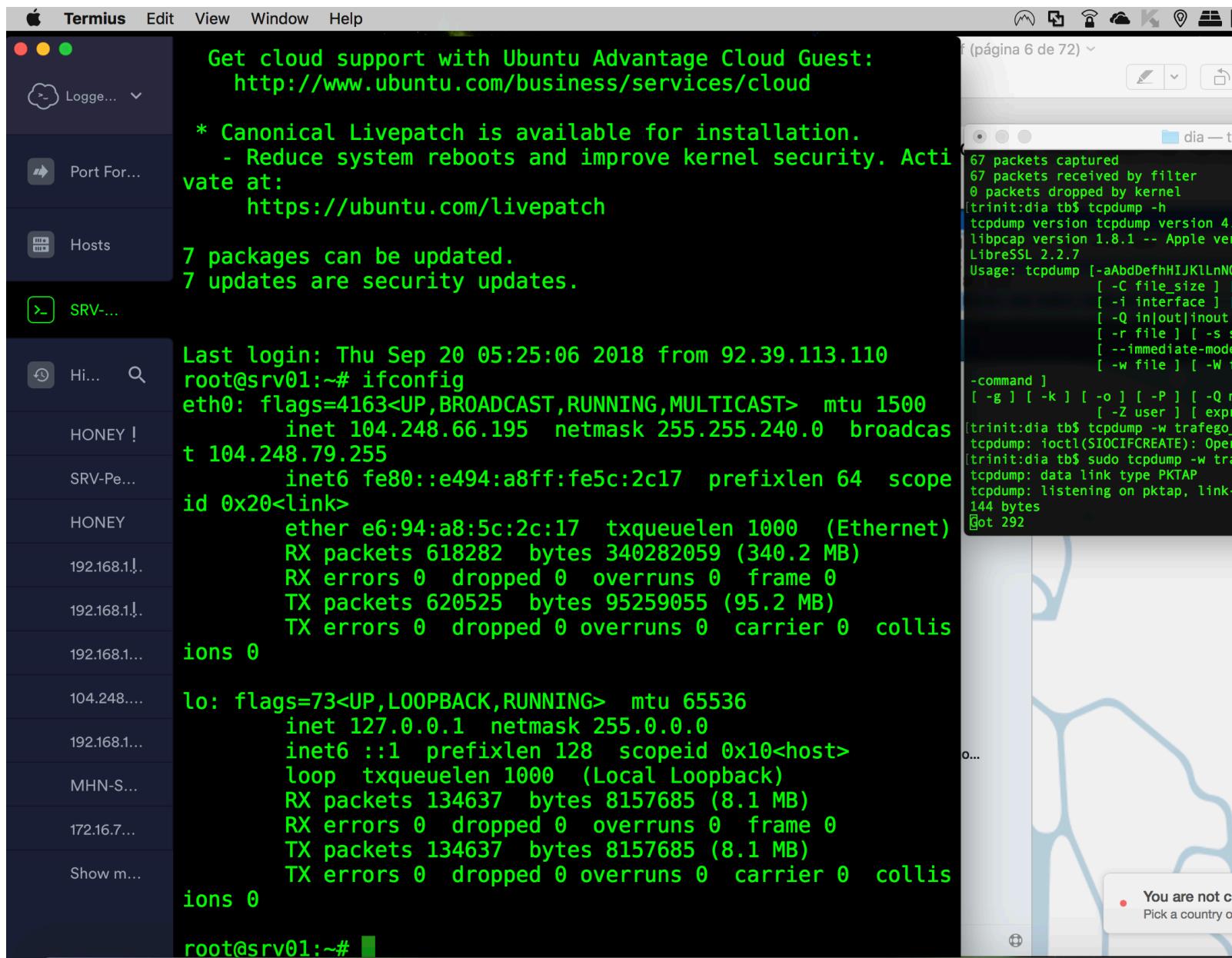
1 - SERIA POSSÍVEL UTILIZAR A INFRAESTRUTURA DE WIFI PARA REALIZAR UM ATAQUE CIBERNÉTICO TENDO COMO ALVO OUTROS EQUIPAMENTOS EXTERNO A INFRAESTRUTURA DA AERONAVE, OU SEJA EQUIPAMENTOS EM SOLO?



2 - SERIA POSSÍVEL ACESSAR EQUIPAMENTOS EM SOLO ATRAVÉS DE ACESSO REMOTO TAIS COMO SSH E REMOTE DESKTOP?

Foi possível estabelecer conectividade com servidores em solo através do protocolo SSH.

Permitindo desta forma que um atacante possa efetuar o “tunelamento” de sua conexão através de outro dispositivo, fazendo com que todo seu acesso a internet não seja monitorado a partir deste momento.



Get cloud support with Ubuntu Advantage Cloud Guest:
<http://www.ubuntu.com/business/services/cloud>

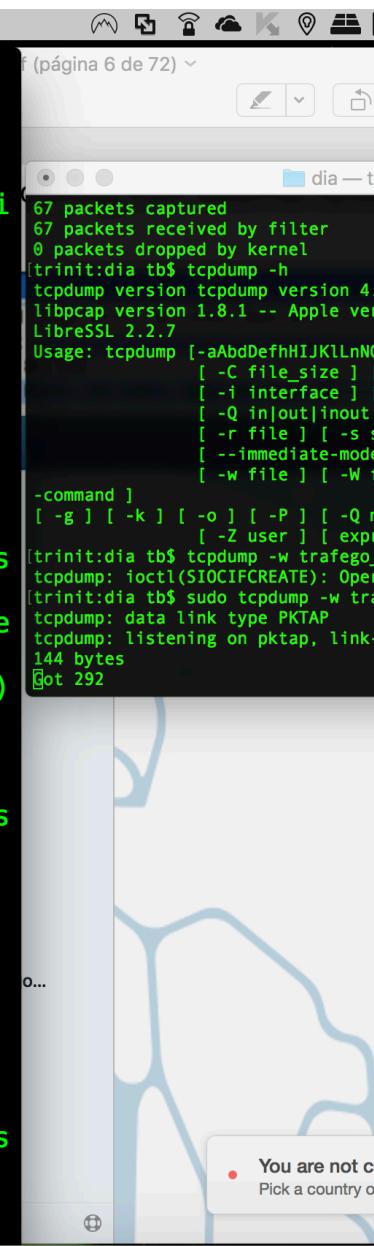
- * Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at:
<https://ubuntu.com/livepatch>

7 packages can be updated.
7 updates are security updates.

```
Last login: Thu Sep 20 05:25:06 2018 from 92.39.113.110
root@srv01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 104.248.66.195 netmask 255.255.240.0 broadcast 104.248.79.255
        inet6 fe80::e494:a8ff:fe5c:2c17 prefixlen 64 scopeid 0x20<link>
          ether e6:94:a8:5c:2c:17 txqueuelen 1000 (Ethernet)
          RX packets 618282 bytes 340282059 (340.2 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 620525 bytes 95259055 (95.2 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 134637 bytes 8157685 (8.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 134637 bytes 8157685 (8.1 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@srv01:~#
```



67 packets captured
67 packets received by filter
0 packets dropped by kernel
[trinith:dia tb\$ tcpdump -h
tcpdump version 4.9.2 libpcap version 1.8.1 -- Apple ve...
LibreSSL 2.2.7
Usage: tcpdump [-aAbDefhHIJKLnNnOoPpRrSsTtVvWw] [-C file_size] [-i interface] [-Q in|out|inout] [-r file] [-s size] [-w file] [-W command] [-g] [-k] [-o options] [-P] [-Q] [-Z user] [-Z group] [exp...
[trinith:dia tb\$ tcpdump -w trafego
tcpdump: ioctl(SIOCIFCREATE): Open
[trinith:dia tb\$ sudo tcpdump -w trafego
tcpdump: data link type PKTAP
tcpdump: listening on ptktap, link layer 144 bytes
Got 292

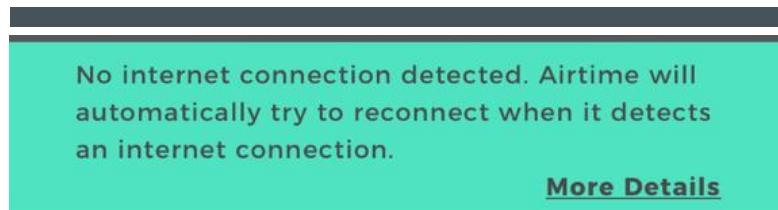
2 - SERIA POSSÍVEL ACESSAR EQUIPAMENTOS EM SOLO ATRAVÉS DE ACESSO REMOTO TAIS COMO SSH E REMOTE DESKTOP?



3 - SERIA POSSÍVEL UM VISITANTE UTILIZAR-SE DE CONTRAMEDIDAS DE PRIVACIDADE AFIM DE PROTEGER OS SEUS ACESSOS E/OU UTILIZAR-SE DESTE SUBTERFUGIO PARA OFUSCAR UM ATAQUE?

Como foi visto anteriormente foi possível realizar tunelamento de tráfego através de um Proxy SSH, outra forma que foi efetivada com sucesso foi a utilização do serviço de VPN onde foi possível estabelecer um acesso a um link de internet no Brasil de forma protegida.

Com isso os filtros de navegação foram bypassados permitindo acessar sites de streaming e de conteúdo não permitido pela política de uso do serviço.



airtime

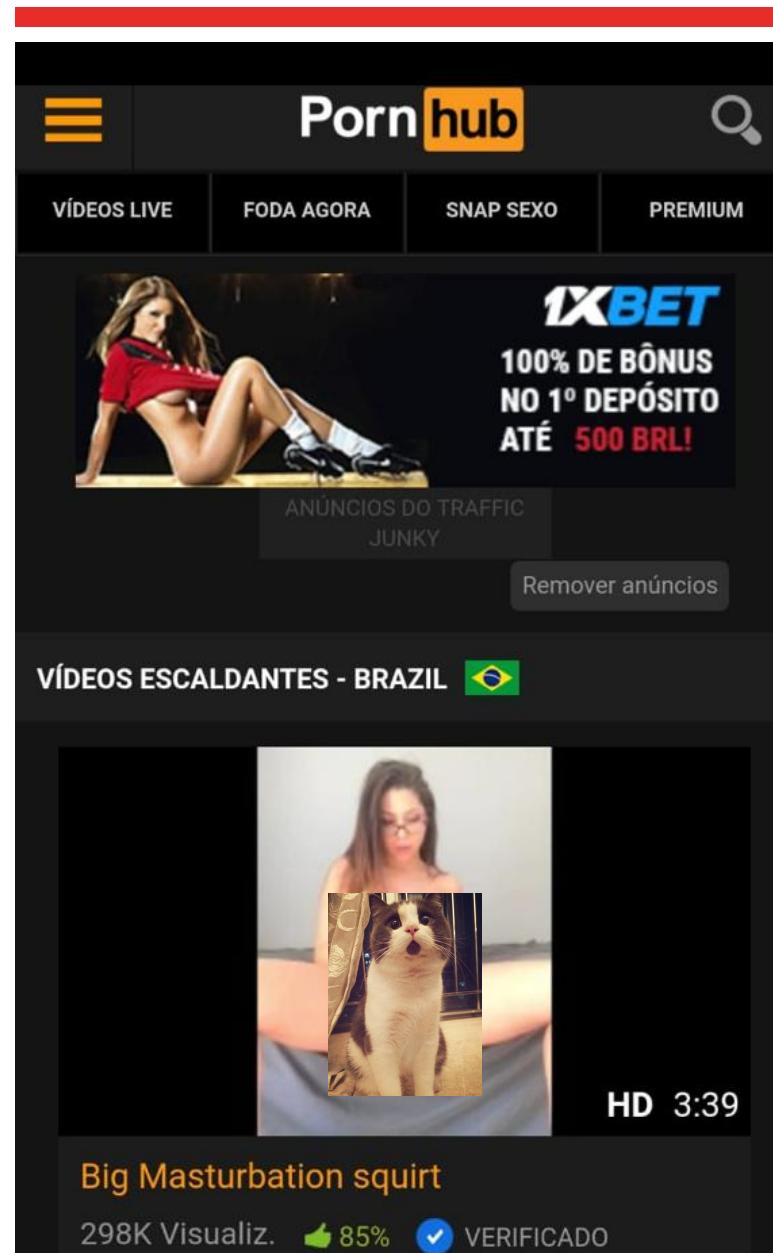
When Can I Use Wi-Fi?

What Can I Do On It?

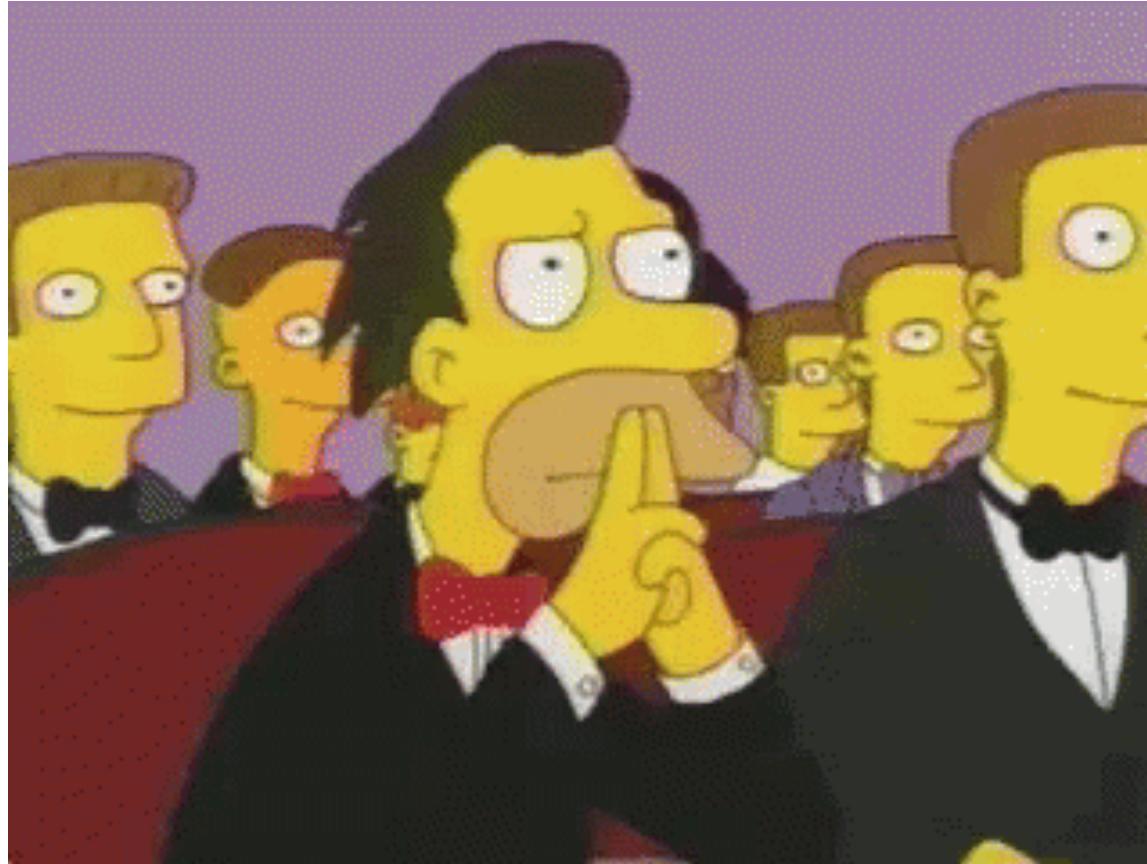
On inflight Wi-Fi, you can do just about anything you can at work and at home. Like other public networks, we restrict inappropriate content and the use of high-bandwidth voice, video and streaming apps. With multiple passengers on the network, performance and speed will vary.

Is My Connection Secure?

Inflight Wi-Fi is similar to public Wi-Fi hotspots at coffee shops, libraries, hotels and airports. You should exercise the same precautions you do on those networks.



3 - SERIA POSSÍVEL UM VISITANTE UTILIZAR-SE DE CONTRAMEDIDAS DE PRIVACIDADE AFIM DE PROTEGER OS SEUS ACESSOS E/OU UTILIZAR-SE DESTE SUBTERFUGIO PARA OFUSCAR UM ATAQUE?

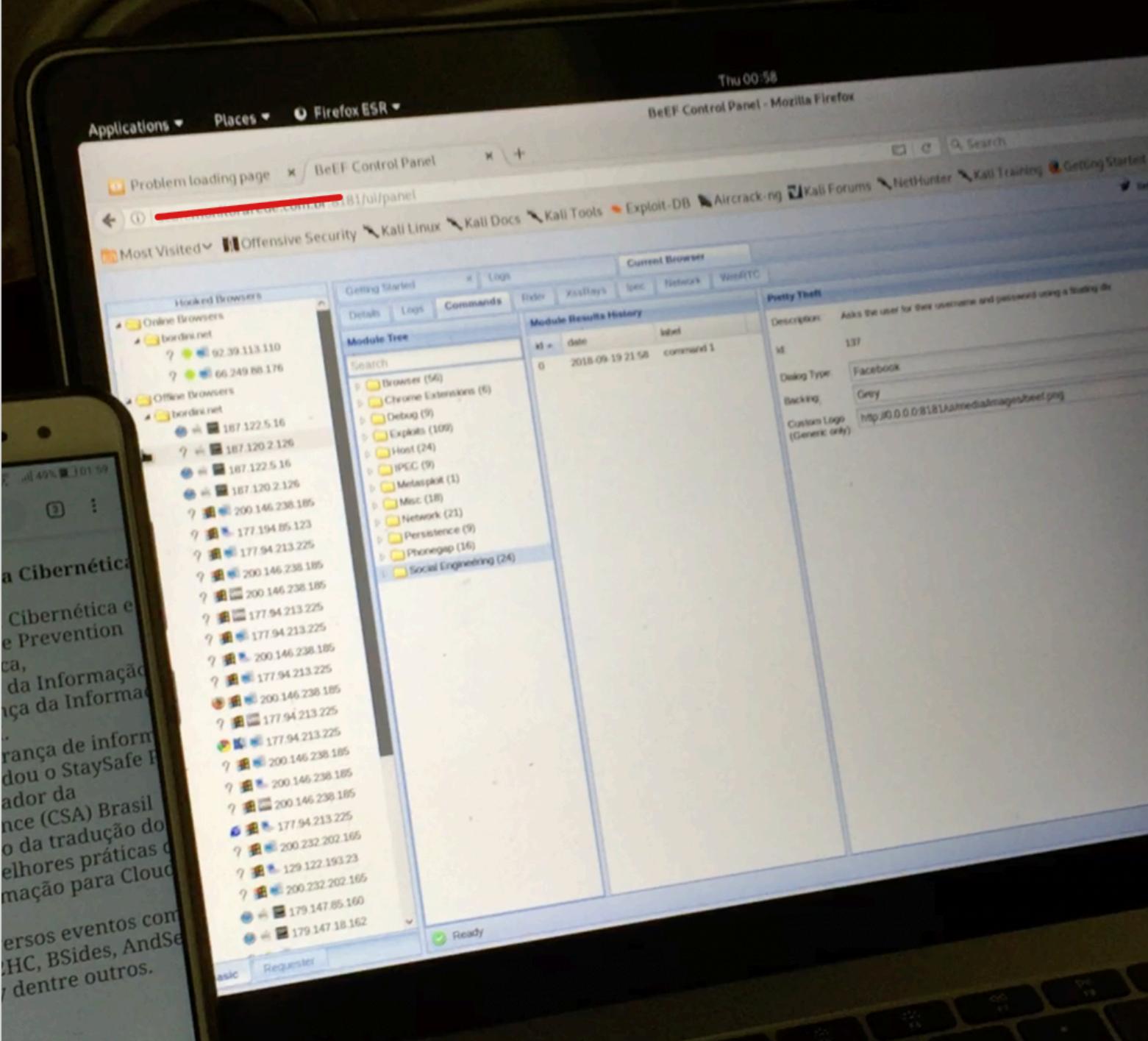


4 - SERIA POSSÍVEL DE SOLO ACESSAR E/OU COMPROMETER UM EQUIPAMENTO CONECTADO NO WIFI DA AERONAVE?

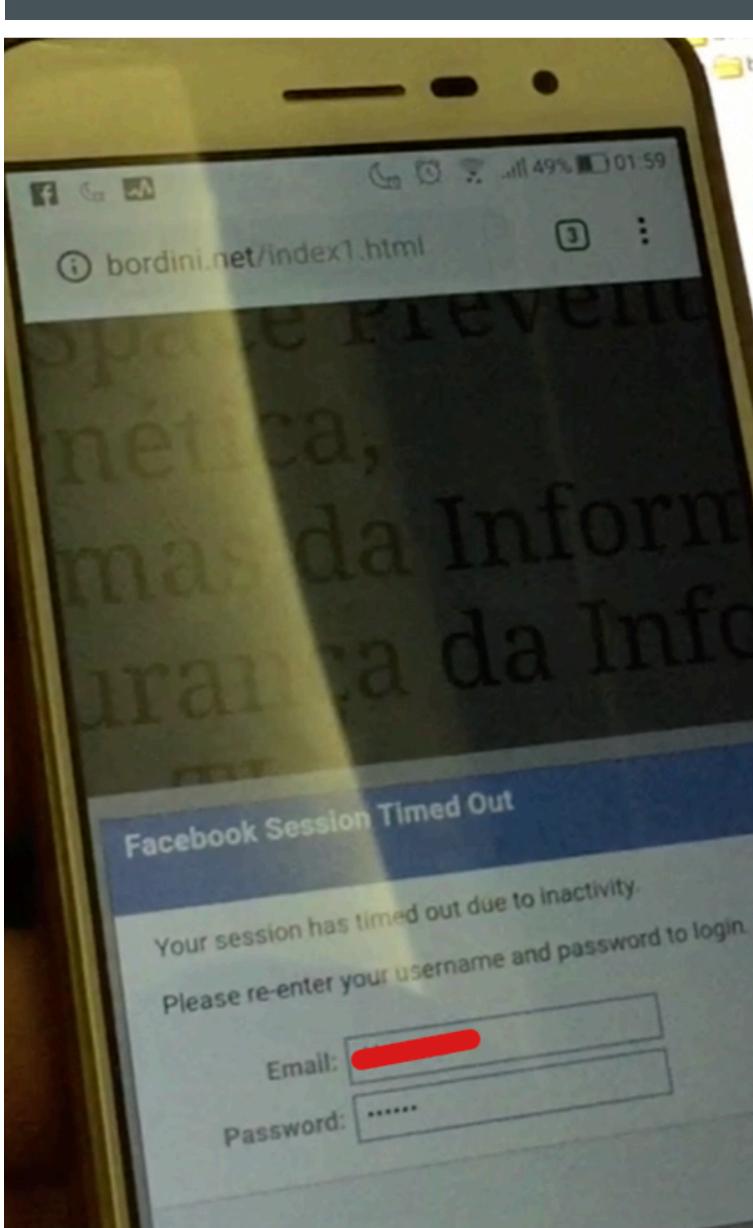
Sim, foi possível através de duas técnicas avaliadas:

A primeira dela consistiu no acesso por parte do usuário a um site com conteúdo malicioso e partir deste modo o atacante conseguiria de solo manipular as requisições no navegador da vítima.

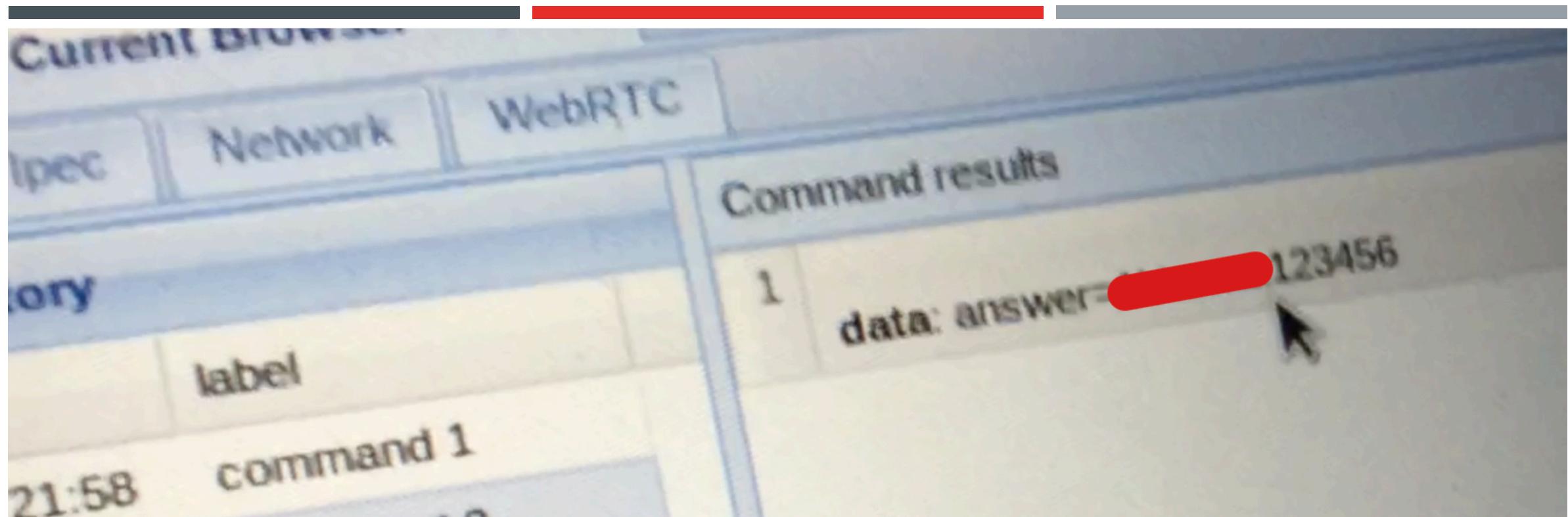
Nos testes foi possível por exemplo exibir uma página falsa do Facebook onde a vítima inseriu seu usuário e senha, e esta informação foi coletada pelo atacante em solo.



4 - SERIA POSSÍVEL DE SOLO ACESSAR E/OU COMPROMETER UM EQUIPAMENTO CONECTADO NO WIFI DA AERONAVE?



PÁGINA INJETADA ATRAVÉS DE
UM C2 EM SOLO RODANDO
BEEF



DADOS DA VÍTIMA COLETADOS EM SOLO

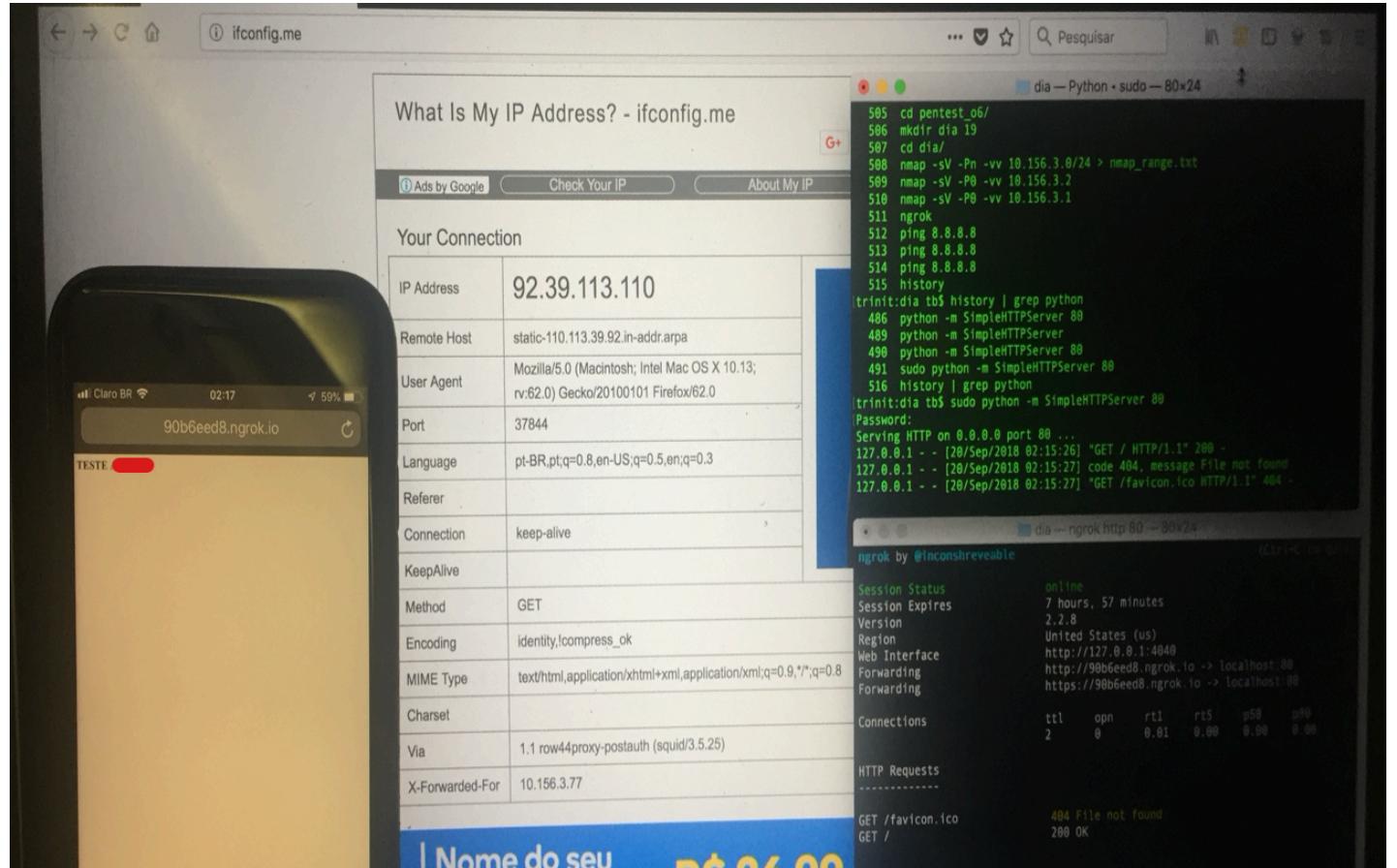
4 - SERIA POSSÍVEL DE SOLO ACESSAR E/OU COMPROMETER UM EQUIPAMENTO CONECTADO NO WIFI DA AERONAVE?

O segundo ataque envolve uma técnica com um risco maior, foi possível iniciar um servidor de páginas em um Raspberry conectado a internet da aeronave e publicá-lo de modo que um atacante em solo conseguiria acesso a este dispositivo, isso comprova que o sistema não tem bloqueios para acessos maliciosos oriundos de uma infraestrutura em solo.



RASPY + PYTHON + NGROK (ONBOARD)

VISITANTE EM
SOLO



CONTE-ME MAIS



SOBRE ISSO

GERAL

RASPBERRY?



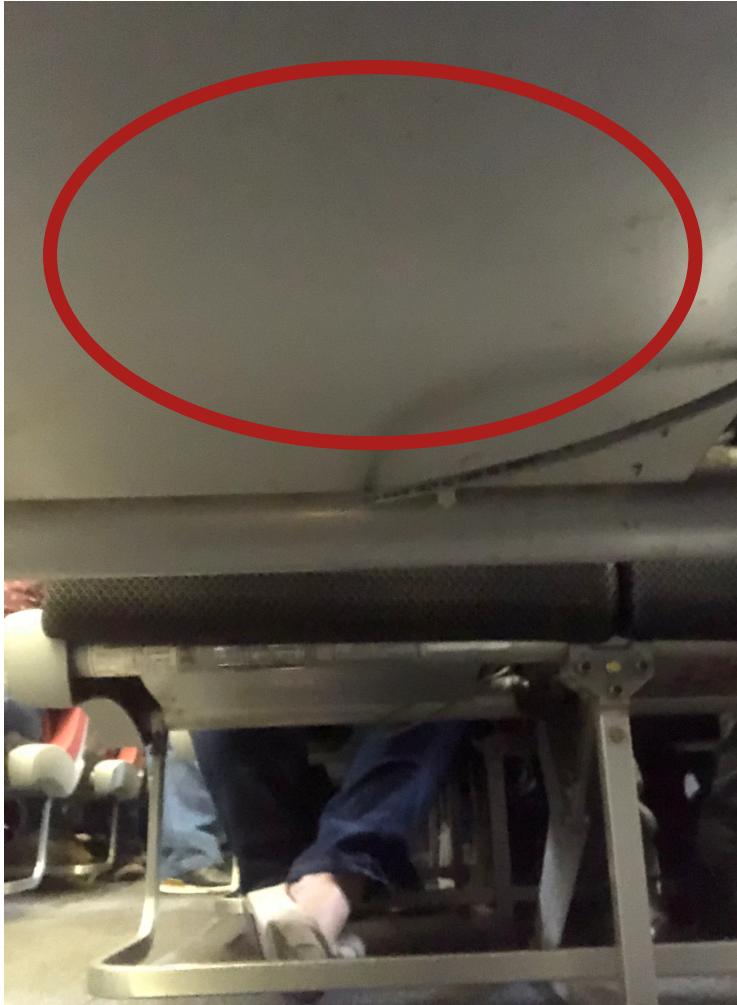


RASPY + POWERBANK

O device foi fixado sob o assento e ficou na aeronave até a noite do dia seguinte quando entramos na aeronave para retirar, durante este período a aeronave fez 14 voos na ponte aérea Rio de Janeiro - São Paulo, permanecendo online por cerca de 12 horas.

Durante este período ninguém detectou o dispositivo, nem após a limpeza geral realizada durante o período noturno com a aeronave em pátio.

PONTOS DE
FIXAÇÃO NÃO
OBSERVADOS



RASPY + POWERBANK



MAS E SE
ENCONTRASSEM
O DEVICE?

— Márcia do céu, corre
aqui. Olha o tamanho
desse carrapato!



O QUE FOI OBSERVADO DURANTE O PERÍODO ATIVO?

Alguns pontos chamaram a atenção como a segmentação de tráfego entre os clientes, foi necessário realizar um arp spoofing para conseguir ter acesso ao tráfego dos demais usuários.

Algo que chamou a atenção foi a quantidade de rádios e redes criadas a bordo.

Foram mapeados 3 rádios cada um deles com 3 redes, sendo estas 1 com BSSID oculto e 2 disponíveis (Passageiros e Tripulação).

FC:0A:81:B5:CA:72	-46	775	0	0	1	130	WPA2	CCMP	PSK	<length: 1>
CH 7]	[Elapsed: 9 mins]	[2018-09-19 22:55								ght
<hr/>										
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:18:84:84:84:84:84:C0:C1:C2:FC:FC:FC	A0:02:00:02:01:-37:-38:-37:-37:-47:-47:-47	-1:-1:-29:-33:-31:-37:-38:-37:-47:-47:-47	0:0:1718:1690:1701:1238:1251:1201:1134:1137:1064	2:2:219:0:0:0:0:0:281:0:0	0:0:1:6:6:11:11:11:1:1	7:-1:-1:130:130:130:130:130:130:130	OPN:WPA:OPN:WPA2 CCMP:WPA2 CCMP:OPN:WPA2 CCMP:WPA2 CCMP:OPN:WPA2 CCMP		PSK:PSK:PSK:PSK:PSK:PSK:PSK:PSK:PSK:PSK	<length: 0><length: 0>airtimeinflight<length: 1>crewnetoneairtimeinflightcrewnetone<length: 1>airtimeinflight

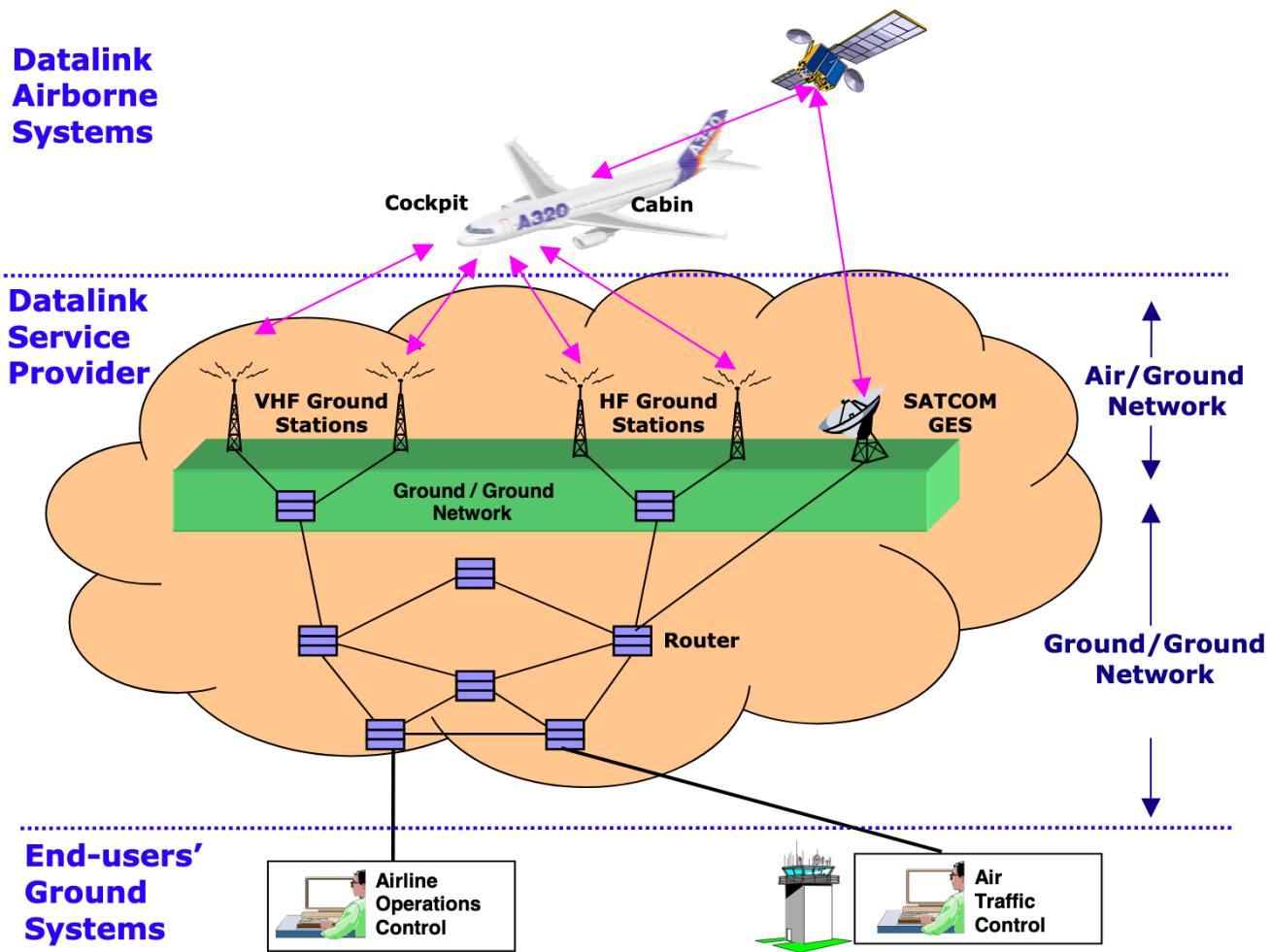
O QUE FOI OBSERVADO DURANTE O PERÍODO ATIVO?

O QUE NÃO FOI TESTADO

Os próximos passos da pesquisa envolvem o comprometimento de outras redes disponíveis (oculta e Tripulação) a fim de verificar quais outros vetores de ataque seriam possíveis.

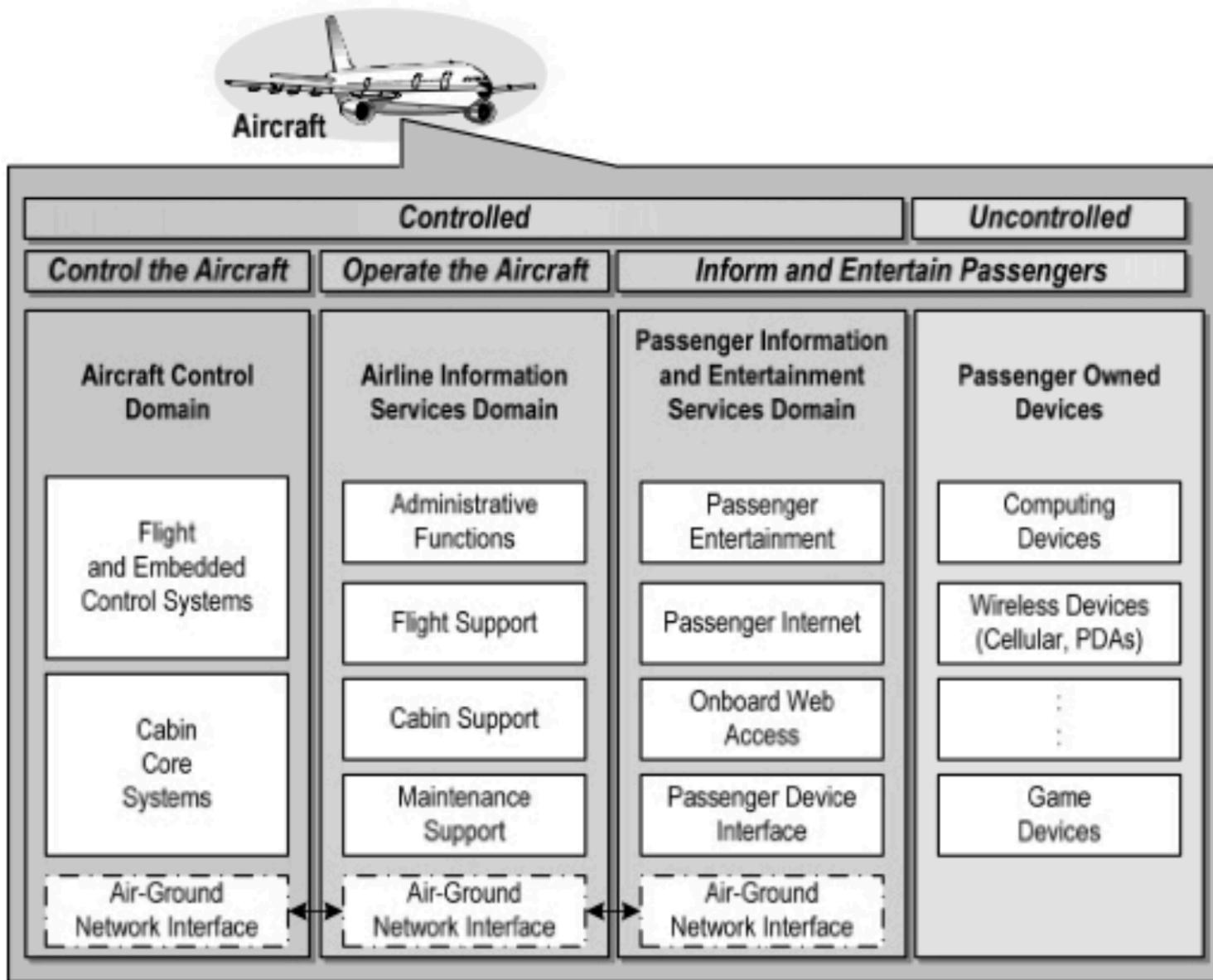
Tentar captura e/ou manipulação no tráfego de dados dos computadores de bordo da aeronave em voo ou em solo, tendo em vista que quando a aeronave esta em solo ocorre o sincronismo dos dados de telemetria com as bases de manutenção e controle da aeronave através de sinais HF e VHF.

Tentar realizar a movimentação lateral entre as redes, tendo vista que existe um canal de comunicação de dados entre sistema wifi, sistema de entretenimento e sistemas de controle de voo e telemetria da aeronave.



PRÓXIMOS OBJETIVOS

DATA INTERCEPT

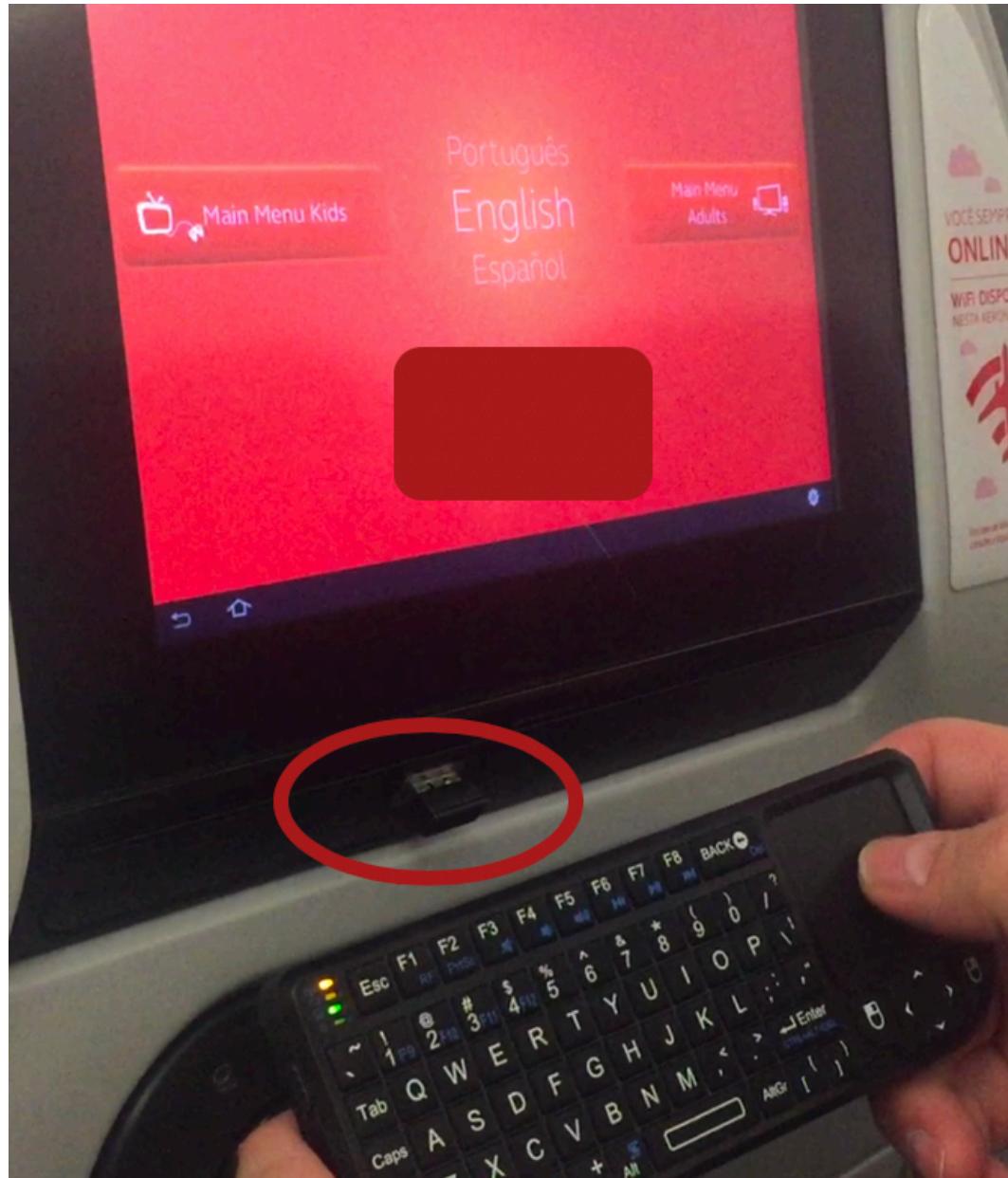


PRÓXIMOS
OBJETIVOS

NETWORK
PIVOT

PRÓXIMOS
OBJETIVOS

USB
CHARGER???



OBRIGADO

Thiago Bordini - @tbordini

Diego Rubio

