OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #5 – PASSWORD CRACKING AND WIFI CRACKING

JEGGO PAOLO V. DYCOK

01242866

Task A: Linux Password Cracking (25 points)

1. 5 points. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.



- I created two groups, cyse301s23 and jdyco001 using groupadd command
- I used the tail command on /etc/group to show the last two groups added

2. 5 points. Create and assign three users to each group. Display related UID and GID information of each user.

	ro	ot@CS2APenTest: ~	0	•	0
	File Edit View Search Terminal Help				
if	root@CS2APenTest:~# useradd Bob				~
6.	root@CS2APenTest:~# useradd Alice				
d€	<pre>root@CS2APenTest:~# useradd May</pre>				
	root@CS2APenTest:~# useradd Sean				
Ì	<pre>root@CS2APenTest:~# useradd John</pre>				
I	<pre>root@CS2APenTest:~# useradd Kim</pre>				
s	root@CS2APenTest:~# usermod -a-G c	yse301s23 Bob			
	usermod: invalid option '-'				
	usage: usermod [options] LUGIN				
	Options:				
	-c,comment COMMENT ne	w value of the GECOS field			
	-d,home HOME DIR new	w home directory for the user account			
	-e,expiredate EXPIRE_DATE se	t account expiration date to EXPIRE_DA	TE		
	-f,inactive INACTIVE se	t password inactive after expiration			
	to	INACTIVE			
	-g,gid GROUP fo	rce use GROUP as new primary group			
	-G,groups GROUPS net	w list of supplementary GROUPS			
	-a,append ap	pend the user to the supplemental GROU	IPS		
	#b	e user from other arouns	ring		
	-hheln di	splay this help message and exit			
	-1login NEW LOGIN new	w value of the login name			
	-L,lock lo	ck the user account			
	-m,move-home mo	ve contents of the home directory to t	the		
	ne	w location (use only with -d)			- 14
	-o,non-unique al	low using duplicate (non-unique) UID			
	-p,password PASSWORD us	e encrypted password for the new passw	ord		
	-R,root CHROOT_DIR di	rectory to chroot into			
	-P,prefix PREFIX_DIR pro	efix directory where are located the /	etc	/*	n
	Les	w login shell for the user account			
	-u,uid UTD net	w UTD for the user account			
	-Uunlock un	lock the user account			
	-v,add-subuids FIRST-LAST ad	d range of subordinate uids			
	-V,del-subuids FIRST-LAST re	move range of subordinate uids			
	-w,add-subgids FIRST-LAST ad	d range of subordinate gids			
	-W,del-subgids FIRST-LAST re	move range of subordinate gids			
	-Zselinux-user SEUSER new	w SELinux user mapping for the user ac	cou	int	

	root@CS2APenTest: ~	•	Θ	0
File Edit View Search Terminal	Help			
-o,non-unique -p,password PASSWORD -R,root CHROOT_DIR -P,prefix PREFIX_DIR	new location (use only with -d) allow using duplicate (non-unique) use encrypted password for the new directory to chroot into prefix directory where are located	UID password the /etc	I ;/*	ŕi
-s,shell SHELL -u,uid UID -U,unlock -v,add-subuids FIRST-LAST -V,del-subuids FIRST-LAST -w,add-subgids FIRST-LAST -W,del-subgids FIRST-LAST -Z,selinux-user SEUSER	new login shell for the user accoun new UID for the user account unlock the user account add range of subordinate uids remove range of subordinate uids add range of subordinate gids remove range of subordinate gids new SELinux user mapping for the us	it er accou	int	
<pre>root@CS2APenTest:=# usermod -G root@CS2APenTest:=# usermod -G root@CS2APenTest:=#</pre>	cyse301s23 Bob cyse301s23 Alice cyse301s23 May jdyco001 Sean jdyco001 John jdyco001 Kim tc/passwd h/sh :/bin/sh h/sh bin/sh bin/sh bin/sh			

- I created 6 users: Bob, Alice, May, Sean, John and Kim.
- I assigned Bob, Alice, and May to cyse301s23. I assigned Sean, John, and Kim to jdyco001. I then used tail –6 command to show UID and GID of all users.

3. 5 points. Choose six new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords.



- I used passwd command to create passwords for all 6 users.
 - Bob pw: 123456789
 - Alice pw: P@ssword123
 - May pw: 0987654321
 - Sean Apple123
 - John KiwiStrawberry123
 - o Kim Mik1234567

4. 5 points. Export all six users' password hashes into a file named "YourMIDAS-HASH" (for example, pjiang-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



root@CS2APenTest: ~	•	•	0
File Edit View Search Terminal Help			
root@CS2APenTest:~# john jdyco001-HASH			-
Using default input encoding: UTF-8			
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) \$6\$ [SHA512 256/256 AVX2 4x])			
Cost 1 (Iteration count) is 5000 for all loaded nashes			
Proceeding with single rules: Single			
Press 'a' or Crl-C to abort, almost any other key for status			
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: only 5 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.			
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.			
Further messages of this type will be suppressed.			
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf			
Almost done: Processing the remaining buffered candidate passwords, if any.			
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist			
123456789 (Bob)			
098/034321 (May)			
			\sim

• I exported all six users to jdyco001-HASH using Nano.

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to

establish a reverse shell connection with the admin privilege to the target Windows 7 VM. Now, complete the following tasks:

1. 5 points. Display the password hashes by using the "hashdump" command in the meterpreter shell. Then

Ben/P@ss12345

Ann/Abc123456

Kat/54321Apple



PROCEDURE:

- I launched a reverse TCP by setting up Kali linux as the listener and msfvenom to deliver a payload to windows 7
- I used command set session 1 and used bypassuac to get administrator access to utilize hashdump command.

2. 10 points. Save the password hashes into a file named "your_midas.WinHASH" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).

	root@CS2APenTest: ~	Ť o	0 0				
File Edit View	Search Terminal Help						
iably			^				
Session complete	d			Tasti		1	100
root@C52APenTest	: # johnformat=NT jdyco001.WinHASH			iiest: ~			1
Using default in	put encoding: UTF-8		International International				
Loaded 7 passwor)	d hashes with no different salts (NT [MD4 51	2/512 AVX512BW	16x3]	root@CS2APenTest: -	×	٠	+
Warning: no Open Proceeding with	MP support for this hash type, considerfo single, rules:Single	ork=2	192.10	217.3:4444			^
Almost done: Pro Warning: Only 4 performance.	cessing the remaining buffered candidate pas candidates buffered for the current salt, mi	swords, if any nimum 48 neede	d for	inuing]			
Proceeding with password Proceeding with 3g 0:00:01:15 3 3g 0:00:02:09 3 3g 0:00:02:09 3 3g 0:00:03:18 3 3g 0:00:03:35 3	<pre>wordlist:/usr/share/john/password.lst, rules (window 7) (Guest) incremental:ASCII /3 0.03927g/s 23334Kp/s 23334Kc/s 9338KC/s /3 0.03528g/s 23632Kp/s 23632Kc/s 94565KC/s /3 0.02325g/s 23798Kp/s 23798Kc/s 95216KC/s /3 0.01514g/s 24155Kp/s 24155Kc/s 96620KC/s /3 0.0159g/s 24171Kp/s 24171Kc/s 96638Kc/s</pre>	:Wordlist v4azl2mariqk fluvl1sfluvc pwoksl03pwok lulvjiclulvn rx8juzrx776	1 08 (sul3 es	the filesystem => long being uploaded 217.2 17.3:4444 -> 192.168.217 51404ee:31d6cfe0d16ae931	.2:5364 b73c590	41) a 17e0c	at :08
3g 0:00:03:51 3	/3 0.01298g/s 24279Kp/s 24279Kc/s 97118KC/s	2mckah712mck	1912	p07t770c2t37e09a850e09e9 10bb8e5bf4aa68fb56a2474e 31d6cfe0d16ae931b73c59d7	20a914: ee2d01: e0c089;	5::: f::: cΘ:::	
	HomeGroupUser\$:1002;aa 44b23::: Kat:1005:aad3b435b514 Window 7:1000:aad3b433 :: meterpreter > []	ad3b435b51484ee 94eeaad3b435b51 5b51404eeaad3b4	eaad3b43 1404ee:2 435b5140	5b51404ee:2d79c7f57c09ba 69a5fed6ff304e709933a6ft 4ee:8846f7eaee8fb117ad06	d3139f: e4dd52l bdd830l	56290 b::: b7586)e4 5c:

• I saved all the hashes to jdyco001.Win-HASH and ran john the ripper for 10 minutes and got 1 password

3. 10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).

Dictionary				
File	Positi	on		
C:\Program Files\Cain\Wordlists\Wordlist.txt	3456	292		
- Key Rate	Options			
Dictionary Position	As is (F Revers Double Duble Duble Duble Duble Duble	RD - DRDWSSAI Pass) /ORD - password rd - PASSWORD	P)))	
Durrent password	Case po Two nu	ab, perms (P. erms (Pass,p mbers Hybric	ass.P4ss.PaosPaSs Ass.paSsPaSs d Brute (Pass0F	P458P458 PASS) Pace99(
			Start	Ext
te-Force Attack			Stat	E si
te-Force Attack Charast © Predelined abcdefghijklinnopgistvavvajc0123456789 © Custom	<u>×</u>	Pasaw Min Max	Start	Ent
e-Force Attack Thorset Predefined abcdefgrijklimnopgistuwwsje0123455789 C. Custom	-	Passov Min Max	Start	Ext
te-Force Attack Predefined abcdefghijklinnopgistvavvajc0123456789 C Custom Keyspace 6.1860514273734411E+024	renk password de	Passw Min Max Start In	Start	Ext
te-Force Attack Thorset © Predefined abcdefghikknnopqistwwwye0123455789 C Custom legspace 8.1660514273734411E+024 Custom	tenk password de ie Left	Passw Min Max Start In Frykd	Start	Ent
te-Force Attack Charact Predefined abcdefghijkimnopgistuwwsje0123455789 Clustom Regspace 8.1860514273734411E+024 Cu Cu Cu Cu Cu Cu Cu Cu Cu Cu	rent password de ie Leit 3 5984e	Passw Min Max Start II Frvkd	Start	Ext

• I uploaded the CAIN and ABEL tool using upload command to upload the setup and ran it, loading the hashes to initiate dictionary attack and brute force.

Task C: 20 points Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.



1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

- I opened the wireshark file, used aircrack to decrypt WEP key and used airdecap-ng to create a decrypted file that shoes the protocols. Found a couple of EAP, ARP, TCP, HTTP. Although, the majority of the packets were ARP packets which make up 86% of all traffic.
- 2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)

		lab4wpa2	2.cap		- 0	×
le Edit View Go (apture Analyze Statisti	cs Telephony Wireless	Tools Help			_
(1 / 0 h	🖹 🕅 🕲 🖉	+ + + 🗐 🗖		**		
				202		
eapol					Expression	
1285 9 788199	Source Discort i Zord@ro	Destination	Protoco *	Length Info 133 Key (Nessage 1	of 4)	
1287 9.710241	Apple_d3:93:65	Cisco-Li_7c:d0:c	7 EAPOL	155 Key (Message 2	of 4)	
1292 9.715358 1294 9.716899	Cisco-Li_7c:d0:c Apple_d3:93:65	7 Apple_d3:93:65 Cisco-Li 7c:d0:c	7 EAPOL	195 Key (Message 3 133 Key (Message 4	of 4)	
1204 0.110000	Mphic_03193103	01000-01_1010010	CAPOC	TOO Well (Heppende a	01 4)	
						•
rame 1285: 133 b	vites on wire (1064 b	<pre>its), 133 bytes captu 2ADepTert =///VSE301/Mov</pre>	red (1064 bl) tale V. Wirelerr S	ts) acuritu	000	-
ile Edit View Sea	rotoges	zarentest. «Jersesozpho	anc 4-4411 cicas a	ecurry	000	
Epoch Tine: 144	7161757.039470000 80	conds			*	- 8
	KEY FOUND!	[password]				- 11
						- 11
Master Key	285: 20 64 DE 6A 2E	73 86 96 81 91 8E 8C	1E 32 49 FC			*
	30 09 04 44 00	20 0C 94 45 40 DF 0F	D9 79 PC 3D			
Transient Ke	y : B8 1C 67 D0 7A	34 96 C6 CD 51 A7 78	C8 F4 77 C2			
	2A 65 A4 C0 A0	D1 4A 96 BC C5 96 65	7A FC A2 44			
	94 14 51 EC 9C	42 51 E1 EA BF AE 5F	BB 64 11 0D			
EAPOL HMAC	: 49 94 2C 92 12	04 BA 66 ED D8 40 0F	10 A5 19 47			
tecs2APenTest	/CYSE301/Module V-Wi	ireless Security# air	decap-ng -p p	assword lab4wpa2.cap		
irdecap-nghel	p" for help.				(D.O%) Profile efau	ilt
ot@CS2APenTest -	/CYSE301/Module V-W	ireless Security# air	decap-ng -p p	assword lab4wpa2.cap	-e CCNI	
tal number of pa	ckets read	13				
tal number of WE	P data packets	19				
tal number of WP mber of plaintex	A data packets t data packets	2284			Activate	NV N
wher of decrypte	d WEP packets	0			Go to Sett	sin X i to
mber of corrupte	d WEP packets d WPA packets	0 2228				1
wher of had TKID	(WDA) nackets	ñ —				
Edit View Go	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephony <u>W</u> ireless]	[ools <u>H</u> elp			
	<u> </u>	* -1 !* * 🖃 📃	્યલ્લ્	#		-11
pply a display filter	<ctrl-></ctrl->				Expression	•
Time	Source	Destination	Protocol	Length Info		-
2 9,933209	Apple_d3:93:65 192.168.2.23	Broadcast 8.8.8.8	DNS	42 Who has 169.254 73 Standard guery	0xcb70 A www.ap	
3 8.227328	192.168.2.23	224.0.0.251	MDNS	156 Standard query	0x0808 ANY Peng	
4 8.227328	192.168.2.23	192.168.2.1 ffe2::1:ffd3:935	UDP 5 TCMPV6	46 58834 → 192 Len 78 Neighbor Soligi	tation for fe88	
6 8.669832	fe80::a65c:60ff:	fed ff02::fb	MDNS	340 Standard query	0x0808 PTR_air	
ame 1: 42 hytes	on wire (236 bits)	42 hytes captured (2	as hits)		P.	-
hernet II, Src:	Apple_d3:93:65 (a4:	5e:68:d3:93:65), Dst:	Broadcast (f	f:ff:ff:ff:ff)		-
dress Resolution) Protocol (request)					
(root@CS2APenTest	:-/CYSE301/Mod	lule V-Wireless Security	6	9 0
File	Edit View Search Ten	minal Help				
off ff ft tt t	Master Kev : 20	64 DE 6A 2E 73 86 96	81 91 8E 8C	1E 32 49 FC		
08 80 08 08 08	0 00 at to tt tt 38	C9 0A 44 BC 28 8E 94	45 48 BF 8F	89 79 FC 38		
	Transient Key 1 88	10 67 08 74 34 96 06	CD 51 47 78	C8 F4 77 C2		
	EE	AE E5 48 5D 7F 5E F5	AA 69 76 D8	85 83 31 FA		
	2A 04	65 A4 C8 A8 D1 4A 96 14 51 EC 90 42 51 E1	BC C5 96 65	7A FC A2 44 BB 64 11 80		
	34	1. 01 00 00 42 01 01	Lex of AL or	00 01 11 00		
1ab4wpa2-080.00	EAPOL HMAC : 49	94 2C 92 12 04 BA 66	ED D8 40 OF	10 A5 19 47 lecan-ng -p password 1	ab4wpa2.cap	
You ni	ist also specify the	ESSID (-e).	una nu a⊻ru	receiping pipassword	can appendap	
lab4wpa2 airda	capinghelp" for	help.	Pa	ckets: 10074 - Displayed: 4 (0.0%) Profile: Defaul	1
Total	number of stations	seen 13	contry# airo	ecaping ip password	Cabawpaz.cap -e CCN1	
Total	number of packets r	ead 10874				
Total Total	number of WEP data number of WPA data	packets 19 packets 2284				
Nunber	r of plaintext data	packets 7			Activate	Wine
Nunber	r of decrypted MEP	packets 0 packets 0			Go to Setti	198 10
indribe!	r of decrypted WPA	packets 2228				
Nunce						

s

root@CS2APenTest: ~/CYSE30	01 0 0
File Edit View Search Terminal Help	
rootgC52APenTest: # cd -/CYSE301 rootgC52APenTest:# aircrack-ng WPA2-P5-01.c Opening WPA2-P5-01.cape wait Read 7675 packets.	cap WPA2-P5-01-dec.cap
# BSSID ESSID E	Encryption
1 00:16:06:DA:CF:2F CyberPHY 8	wPA (1 handshake)
Choosing first network as target.	Destination Protoco
Opening WPA2-P5-01.cape wait Read 7675 packets.	199.26 192.148.1.127 TCP FF02:18 ICMPv 255.255.255 DHCP
1 potential targets	255.255.255.255 DHCP .98.188 192.168.1.127 TLSV1
Please specify a dictionary (option -w). restances of the second	28 bits), 66 bytes captured (528 bits) is:ef:2d (00:16:b6:da:ef:2d), Dst: Huuwel Sre: 60-205.100-2d, Dst: 192.160.1.127 1, Sre Port: 8900, Dst Port: 40280, Seq: 1, Sre Port: 8900, Dst Port: 40280, Seq:
Module IV- Password Wireless Cracking Security	4 ************************************
	⊘ 2 WPA2-P5-01-dec.cap Packets: 1668 · Displayed: 1668 (100.0%)

			r	oot@CS2APen	Fest: ~/CYSE3	01		•	0	Θ	0			
File	Edit View	Search	Terminal	Help										
root Open Read	OCS2APenTe ing WPA2-P 7675 pack	<mark>st:+/CY</mark> 5-01.ca ets.	<mark>SE301</mark> #∖äi pe wait	rcrack-ng V 	IPA2-P5-01.	cap -w	rockyoı	J.txt			^			
#	BSSID		ESSID			Encrypt:	ion							
1	00:16:B6	:DA:CF:	2F Cyber	РНҮ		WPA (1)	handsha	ake)			L		- 0	
Choo	sing first	networ	k as targ	jet. De Edit								y <u>W</u> ireless <u>T</u> ools <u>H</u> elp		
0pen Bead	ing WPA2-P	5-01.ca	pe wait								H	* _ @ @ @	R 🎹	
Neau	7075 pack												- T P Expression ocol Length .11 10 .11 10 .11 10 .11 10 .11 10 .11 0 .11 0 	
1 po	tential ta	rgets										tion Protoco	Length	
												c8:dd:46 (78: 802.11	10	
												C8:00:46 (78: 802.11 Te b8:3d:23 (802.11	10	
				Aircrack-n	1.5.2							Te_b8:3d:23 (802.11	10	
	[00:00:6	4] 2272	8/7120712	keys teste	d (5026.02	k/s)						·Li_da:cf:2f (802.11	10	
	-			(Þ	
	Time Let	τ: 23 M	inutes, 3	2 seconds				0.32%				aptured (80 bits)		
Hom	CYSE30	1 -	KEY	FOUND! [r	nessenger]	0.		:: • I	_		-	x		
					_				_					
				=	01010 01103 01110		1010 9103 9310							
	Modul	e IV- vord	Module V- Wireless	rockyou.txt	WPA2-P5 01.cap	- WP/ 01-d	A2-P5- lec.cap					·····d··r V·		_
	Crac	ang	Security											





- First, I opened the lab4wpa2.cap and see the encrypted traffic under 802.11
- I used aircrack-ng lab4wpa2.cap
- I selected "4" as an option due to WPA encryption
- I copied rockyou.txt.gz to working directory
- I unzipped rockyou.txt.gz

- I used the file to run a dictionary attack and found the password which is "password"
- I used aircdecap to create lab4wpa2-dec.cap and opened it on wireshark
- By analyzing the file, it appears that majority of the packets are TCP packets which is about 98% and IPV4 packets at 99.7%.

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored

from this encrypted traffic file. -10 points Last digit of your MD5 Filename 0~3 WPA2-P1-01.cap 4~5 WPA2-P2-01.cap 6~8 WPA2-P3-01.cap 9~B WPA2-P4-01.cap C~F WPA2-P5-01.cap

Figure 1 Command to get the MD5 hash.



Be Edit Yew Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Computer Analyze Statistics Telephony Wireless Tools Tool							WPA2	-P5-01	dec.cap			0 0	0 6
Image Image <thimage< th=""> <thimage< th=""> <thim< td=""><td>File</td><td>Edit View Q</td><td><u>5</u>o <u>C</u>apture</td><td><u>A</u>nalyze</td><td>Statistics</td><td>Telephon</td><td><u>W</u>ireles</td><td>s <u>T</u>oo</td><td>ls <u>H</u>elp</td><td></td><td></td><td></td><td></td></thim<></thimage<></thimage<>	File	Edit View Q	<u>5</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	Telephon	<u>W</u> ireles	s <u>T</u> oo	ls <u>H</u> elp				
Apply a display filter Expression a. Time Source Destination Protocol Length Info a. 9.080806 60.285.199.26 192.168.1.127 TCP 66.89969 - 48286 [FIN, ACK] Segn1 Ack=1 is a. 0.080623 :: ff02:168 ICMPv6 130 Multicast Listener Report Message v2 a. 0.135168 0.0.0.0 255.255.255.255 DNCP 366 DNCP Delscover - Transaction ID 0x1277 5.0.220160 108.177.98.188 192.108.1.127 TLSV1.2 97 Application Data Transaction ID 0x1277 5.0.220160 108.3077.98.188 192.108.1.127 TLSV1.2 97 Application Data Transaction ID 0x1277 7.0.302604 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 208.54.65.1097 rell 192.168.1.1 9.0.309772 192.168.1.1 192.168.1.127 192.168.1.1 DNS 49 Standard query 0x838 A connectivity 10.332856 192.168.1.127 192.168.1.127 DNS 49 Standard query 0x838 A connectivity 11.0.323292 21.66.25.9.39.3195 192.168.1.127 DNS 43 Standard query 0x838 A connectivity 11.0.303355 192.168.1.127		■ ⊿ ●	ð 🗎 🖹	۵ م	. + +	.J I≢	+		ଇ୍ପ୍	Q	••		
o. Time Source Destination Protocol Length Info 1 0.0000023 11 1707 66 8980 - 40280 [FIN, ACK] Seg-1 Ack-1 w 2 0.000023 11 1707 68 8980 - 40280 [FIN, ACK] Seg-1 Ack-1 w 3 0.135168 0.0.0 255.255.255.255 DHCP 336 BDCP Discover - Transaction ID 0x1271 5 0.220160 108.177.98.188 192.108.1.127 TLSV1.2 97 Application Data 6 0.20001 108.177.98.188 192.108.1.127 TLSV1.2 97 Application Data 7 0.302664 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 208.54.65.51007 Tell 192.168.1. 8 0.300224 Cisco-Li dat.fr:2d HuaweiTe_b8:3d:23 ARP 42 Who has 208.54.45.51007 Tell 192.168.1. 9 0.309772 192.168.1.127 192.168.1.127 DNS 99 Standard query 0x6398 A connectivity 10 0.325856 192.128.1.127 192.168.1.127 DNS 74 Standard query 0x6203 A www.google.co 12 0.407052 216.58.133.195 HTP 266 GT /generate_204 HTP/1.1 140.414732 13 0.40910 192.168.1.127 DTC 60 Go 402 (2	A	oply a display filt	ter <ctrl-></ctrl->									Expression.	. 4
1 0.000533 1192.168.1.127 TCP 66.8969 - 40226 [FIN, ACK] Seg1 AcK-1 W 2 0.000533 11 ff62:16 ICMPV6 136 Multicast Listener Report Message V2 3 0.135168 0.0.0.0 255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x127h 4 0.44442 0.6.6.8 255.255.255 DHCP 366 DHCP Request - Transaction ID 0x127h 5 0.220160 168.177, 98.188 192.168.1.127 TLSV1.2 97 Application Data 6 0.242664 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 206.54.65.1007 Tell 192.168.1.1 8 0.380224 Cisco-Li_da:cf:2d HuaweiTe_b8:3d:23 ARP 42 Who has 192.168.1.1 11 192.168.1.1 16 0.320564 HuaweiTe_b8:3d:23 ARP 42 Buh has 206.54.65.1007 Tell 192.168.1.1 10 17 0.32.168.1.127 192.168.1.1 192.168.1.1 DNS 89 Standard query Pso308 A connectivity 18 0.325562 192.168.1.127 172.217.5.68 TLSV1.2 588 Cient Hello 19 0.366572 192.168.1.127 172.217.5.68 TLSV1.2 588 Cient Hello <	No.	Time	Sour	ce		Destina	tion		Proto	col	Length	Info	_
2 0.000523 :: ff02:16 ICPP-0 350 DHCP 3		1 0.00088	60.2	205.109.	.26	192.16	58.1.127		TCP		66	8900 → 48280 [FIN, ACK] Seq=1 Ack=1 W	_
3 0.135168 0.0.0.0 255.255.255 DHCP 355 DHCP Discover - Transaction ID 0x127h 5 0.220160 108.177.98.188 192.108.1.127 TLSV1.2 97 Application Data 00x127h 6 0.249860 HuawelTe_D633d:23 Broadcast ARP 42 Who has 200.545.5007 Tell 192.168.1.1 7 0.302604 HuawelTe_D633d:23 Broadcast ARP 42 Who has 192.168.1.117 Tell 192.168.1.1 8 0.308224 Cisco-Lida:cf:2d HuawelTe_D633d:23 ARP 42 192.108.1.1 is at 00:10:10:dic:dic:dic:dic:dic:dic:dic:dic:dic:dic		2 0.00052	23 ::			ff02:	16		ICMP	v6	130	Multicast Listener Report Message v2	
4 0.14643 0.0.0 255.255.255 DHCP 368 DHCP Request - Transaction ID 0x127 5 0.220100 108.177.98.188 192.108.1.127 TLSV1.2 368 DHCP Request - Transaction ID 0x127 7 0.302664 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 192.108.1.115 1192.108.1.1 8 0.308224 Cisco-Li datcf:2d Broadcast ARP 42 Who has 192.108.1.1 1192.108.1.1 9 0.309772 192.108.1.1 192.108.1.1 DNS 89 Standard query 0x0308 A connectivity 10 0.323596 192.108.1.1 DNS 105 Standard query 0x0308 A connectivity 102.108.1.127 11 0.323596 192.108.1.127 192.108.1.127 TCP 66 80 - 41422 [SYN, AcK, Seq=0 Ack=1 Win 13 0.409100 192.168.1.127 172.217.5.68 TLSV1.2 583 Client Hello 16 0.6108050 192.108.1.127 172.217.5.68 TLSV1.2 583 Client Hello 16 0.6108051 192.108.1.127 172.217.5.68 TLSV1.2 583 Client Hello 16 0.6095872 172.217.5.63 192.108.1.127 TCP 66 [TCP ACKed unseen segment) 443 - 4633 17 0.774208 192.108.1.127 192.108.1.127 TSP		3 0.13516	58 0.0	.0.0		255.25	55.255.25	55	DHCP		356	DHCP Discover - Transaction ID 0x127b	
5 0.220100 108.177.98.188 192.108.1.127 TLSV1.2 97 Application Data 6 0.249806 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 208.54.65.1007 Tell 192.108.1 8 0.390784 HuaweiTe_b8:3d:23 Broadcast ARP 42 Who has 192.168.1.11 Tell 192.168.1.1 8 0.390772 192.168.1.127 192.168.1.11 DNS 89 Standard query 9x0398 A connectivity 10 0.312832 192.168.1.127 192.168.1.1 DNS 74 Standard query 9x0398 A connectivity 10 0.312832 192.168.1.127 192.168.1.1 DNS 74 Standard query 9x0398 A connectivity 11 0.407052 216.58.193.195 192.168.1.127 TCP 66 80 - 41492 [SYN, ACK] Seq=0 Ack=1 Win 12 0.407052 216.58.193.195 192.168.1.127 T72.217.5.68 TLSV1.2 583 Client Hello 15 0.618505 192.168.1.127 172.217.5.68 TLSV1.2 583 Client Hello 143 - 4655 16 0.695672 172.217.5.68 192.168.1.127 TOP 66 TCP pencetac_204 HTTP/1.1 140 - 4635 18 0.499443 192.168.1.127 192.168.1.127 TOP 66 TCP Acked unseen segment not capturee] 160 19 0.893515 <td< td=""><td>L</td><td>4 0.14643</td><td>32 0.0</td><td>.0.0</td><td></td><td>255.25</td><td>55.255.25</td><td>55</td><td>DHCP</td><td></td><td>368</td><td>DHCP Request - Transaction ID 0x127b</td><td>_</td></td<>	L	4 0.14643	32 0.0	.0.0		255.25	55.255.25	55	DHCP		368	DHCP Request - Transaction ID 0x127b	_
6 0.249966 HuawelTe_D8:3d:23 Broadcast ARP 42 Who has 200.54.65.1007 Tell 192.168.1.1 8 0.308224 Cisco-Li_da:cf:2d HuaweiTe_D8:3d:23 ARP 42 192.168.1.1 Tell 192.168.1.1 9 0.309772 192.168.1.1.27 192.168.1.1 DNS 89 Standard query 0x9398 A connectivity 10 0.312632 192.166.1.127 192.168.1.1 DNS 105 Standard query 0x9398 A connectivity 11 0.323596 192.166.1.127 192.168.1.1 DNS 74 Standard query 0x9398 A connectivity 13 0.409100 192.166.1.127 192.168.1.1 DNS 74 Standard query 0x928 A connectivity 13 0.409100 192.166.1.127 192.168.1.1 DNS 74 Standard query 0x928 A connectivity 14 0.414732 192.168.1.127 TCP 66 80 - 41492 [SYN, ACK] Seq=0 Ack=1 Win 13 0.409100 192.168.1.127 172.217.5.68 TLSV1.2 S32 [IGT Perevious segment not captured] 16 0.638050 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x464 A AwA nobao.cc 19 0.993515 192.168.1.127 192.168.1.127 DNS 74 Standard query 0x464 A AwA nobao.cc 12 0.906731 192.168.1.127 66.190.24.243 TCP		5 0.22010	50 108	.177.98.	.188	192.1	38.1.127		TLSv	1.2	97	Application Data	
7 0.302604 Huawelle_D8:30:23 Broadcast ARP 42 Who has 192.168.1.1 is at 00:16:b6:di.17 9 0.309772 192.168.1.127 192.168.1.1 DNS 89 Standard query 0x0398 A connectivity 10 0.312032 192.168.1.1 DNS 195 Standard query 0x0398 A connectivity 11 0.323596 192.168.1.127 192.168.1.127 DNS 195 Standard query 0x62b3 A www.gogle.co 12 0.407052 210.58.103.195 192.168.1.127 TCP 66 80 - 41492 (SYM, ACK) Seq=0 Ack=1 Win 13 0.409100 192.168.1.127 172.217.5.68 TLSV1.2 583 Standard query 0x62b3 A www.gogle.co 16 0.6198050 192.168.1.127 172.217.5.68 TLSV1.2 583 Standard query 0x62b3 A www.gogle.co 16 0.6198050 192.168.1.127 172.217.5.68 TLSV1.2 583 Standard query 0x62b3 A www.gogle.co 16 0.6198050 192.168.1.127 172.217.5.68 TLSV1.2 583 Standard query 0x62b3 A www.gogle.co 16 0.6198051 192.168.1.127 192.168.1.127 DNS 168 Standard query 0x62b3 A m.qo 16 0.6198054 192.168.1.127 192.168.1.127 DNS 74 Standard query 0x16da A www.taobao.co 19 0.893515 192.168.1.127 192.168.1.127		6 0.24986	58 Huav	weiTe_b8	8:3d:23	Broad	cast		ARP		42	Who has 208.54.65.100? Tell 192.168.1	
8 0.308224 C1sco-L1_datC1:20 Hukker10_D8:30:23 AAP 42 192.108.1.1 1s at 00:10:00:01:01:01:01:01:01:01:01:01:01:0		7 0.30260	94 Huav	weiTe_b8	8:3d:23	Broad	cast		ARP		42	Who has 192.168.1.1? Tell 192.168.1.1	
9 0.3097/2 192.108.1.127 192.108.1.127 DNS 205 Standard query exosos & 0x308 A connectivity of 0x0308 A c		8 0.30822	24 C150	co-L1_da	a:cf:2d	Huawe:	LTe_b8:3d	1:23	ARP		42	192.168.1.1 is at 00:16:b6:da:cf:2d	
10 0.312032 192.100.1.1 192.100.1.127 DNS 100 Standard query 0x5038 A www.google.co 12 0.407052 216.58.193.195 192.108.1.127 TCP 66 80 - 41492 [SYN, ACK] Seq=0 Ack=1 Win 13 0.4071632 216.58.193.195 192.108.1.127 TCP 66 60 - 41492 [SYN, ACK] Seq=0 Ack=1 Win 14 0.414732 192.108.1.127 172.217.5.68 TLSV1.2 538 Client Hello 15 0.605072 172.217.5.60 192.168.1.127 TCP 66 66 T/generate_204 HTTP/1.1 16 0.605072 172.217.5.60 192.168.1.127 TCP 66 TSP Acked unseen segment not captured], 160 0.050072 17 0.774280 192.168.1.127 192.168.1.127 TCP 66 TSP Acked unseen segment] 443 - 4653 17 0.774280 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x1643 AAAA myow, align 20 0.931463 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x1643 AAAA myow, align 21 0.94886 192.168.1.127 192.168.1.127 TCP 74 44356 - 460 [SYN] Seq=0 Wine5555 Len 21 0.94886 192.168.1.127 192.168.1.127 TCP 74 43170 - 443 [SYN] Seq=0 Wine5555 Len 22 0.906731 192.168.1.127 192.168.1.127<		9 0.30977	72 192	.108.1.1	127	192.10	38.1.1		DNS		89	Standard query 0x0398 A connectivityc	
110.325980 192.106.1.127 192.106.1.127 TCP 66 60 - 41492 192.106.1.127 130.409100 192.106.1.127 216.56.193.195 HTTP 286 6ET /generate_204 HTTP/1.1 140.414732 192.106.1.127 216.56.193.195 HTTP 286 6ET /generate_204 HTTP/1.1 150.409100 192.106.1.127 172.217.5.68 TLSv1.2 382 Client Hello 150.40952 192.106.1.127 172.217.5.68 TLSv1.2 312 [FCP Provious segment not captured], 43 - 4653 170.774288 192.106.1.127 192.106.1.127 DNS 166 Standard query exideA A www.tabbao.co 180.899443 192.106.1.127 192.108.1.1 DNS 84 Standard query exideA A Aww.tabbao.co 280.93515 192.106.1.127 66.190.24.243 TCP 74 49316 - 463 [SVN] Seq=0 Win=5535 Len 210.934880 192.106.1.127 66.190.24.243 TCP 74 49316 - 463 [SVN] Seq=0 Win=5535 Len 210.948806 192.106.1.127 TCP 54 60 - 40356 [ACK] Seq=1 Ack=61 Win=29 211.92253 66.190.24.243 TCP 74 49316 - 443 [SVN] Seq=0 Win=5535 Len 220.960731 192.106.1.27 TCP 74 49316 - 4435 [SVN] Seq=6 Ack=61 Win=29		10 0.31283	32 192	.108.1.1	1	192.10	08.1.12/		DNS		105	Standard query response 0x0398 A conn	_
13 0.407602 210.55.193.30 192.100.1.127 105.51.193.195 HTP 206 0ET /generate_204 HTP/1.1 14 0.414732 192.108.1.127 172.217.5.68 TLSV1.2 538 Client Hello 16 0.618050 192.108.1.127 172.217.5.68 TLSV1.2 538 Client Hello 16 0.618050 192.108.1.127 172.217.5.68 TLSV1.2 538 Client Hello 17 0.774208 192.108.1.127 TGP. Pecvious segment not captured] 443 - 4653 17 0.774208 192.108.1.127 TDP. 108 66 [TCP ACKed unseen segment] 443 - 4653 19 0.893515 192.108.1.127 192.108.1.127 DNS 74 Standard query 0x46da AwAw.taobao.co 20 0.906731 192.108.1.127 192.108.1.127 GO (192 - 0x4635 - 0x66) 535 Len- 21 0.94880 192.108.1.127 192.108.1.127 GO (192 - 0x4635 - 0x66) Standard query 0x46da AwA myw.alipp 21 0.904731 192.108.1.127 192.108.1.127 TCP 74 44356 - 408 [SW] Seq=0 Win=65535 Len 22 0.906731 192.108.1.127 TCP 74 44356 - 404 [SW] Seq=0 Win=65535 Len 24 194888 192.108.1.327 TCP 54 005 - 40356 [AcKC] Seq=1 Ack=61 Win=29 24 19		12 0 40705	10 192	59 102	105	192.10	30 1 127		TCD		66	Standard query 8x6203 A WWW.google.co	
13 0.493100 192.100.1.127 210.50.153.133 MTFP 200 0E 1102.100.1.127 14 0.414732 192.168.1.127 172.217.5.68 TLSV1.2 312 [TCP Previous segment not captured] , 100.059072 16 0.695072 172.217.5.68 TLSV1.2 312 [TCP Previous segment not captured] , 4653 17 0.774288 192.168.1.127 T72.217.5.68 TLSV1.2 312 [TCP Previous segment not captured] , 4633 17 0.774288 192.168.1.127 T02.168.1.127 DNS 74 standard query esponse 0x4cb5 A m. np 18 0.893515 192.168.1.127 192.168.1.1 DNS 74 standard query 0x4643 AAA mygw. alipa 20 0.905731 192.168.1.127 198.11.186.81 TCP 74 43170 - 443 [SVN] Seg=0 Win=05535 Len 21 0.948800 192.168.1.127 198.11.186.81 TCP 74 443170 - 443 [SVN] Seg=0 Win=05535 Len 22 0.960731 192.168.1.127 198.11.186.81 TCP 74 443170 - 443 [SVN] Seg=0 Win=05535 Len 23 1.022539 66.199.24.243 HTTP 114 HEAD / HTTP/1.1 123 1.02253 Len 24 1.94488 192.168.1.127 TCP 54 400 - 40356 [ACK] Seg=1 Ack=61 Win=29 24 1.94488 192.168.1.127 TCP 74 443 - 44376 [SVN] ArxH Same Ac		13 0 40705	102 210	168 1 1	127	216 50	2 102 105		UTTP		286	CET /generate 204 HTTD/1 1	
19 0.4102 192.100.1127 172.217.5.68 122.100.1127 172.217.5.68 122.100.1127 160.695072 172.217.5.68 192.100.1127 172.217.5.68 192.100.1127 160.695072 172.217.5.68 192.100.1127 172.217.5.68 192.100.1127 160.695072 172.217.5.68 192.100.1127 172.217.5.68 192.100.1127 160.65507 162.102.102 166 TCP Previous segment not captured], 66 TCP Previous segment not captured], 160.695072 172.217.5.68 192.100.1127 172.217.5.68 1127.102.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 102.100.1127 104.102.043 102.100.1127 102.100.1127 104.43176 - 4435 [SYN] Seq=0 Win=05555 Len= 21 0.9045031 192.100.1.127 198.11.186.81 TCP 74.43376 - 4435 [SYN] Seq=0 Win=05555 Len= 123.1022539 66.190.24.243 192.100.1.127 TCP 54.00 40356 [ACK] Seq=1 Ack=61 Win=29 24.1 91488 198.11 186.81 127 TCP 74.43376 58.94 Kes on Wire (2944 bits), 368 bytes captured (2944 bits) 114.140.0 / HTP/1.1 123.1022539 <td></td> <td>14 0 41473</td> <td>192</td> <td>168 1 1</td> <td>127</td> <td>172 2</td> <td>7 5 68</td> <td>,</td> <td>TLSV</td> <td>1 2</td> <td>583</td> <td>Client Hello</td> <td></td>		14 0 41473	192	168 1 1	127	172 2	7 5 68	,	TLSV	1 2	583	Client Hello	
16 0.00000 107.301.11.1 117.11.1		15 0 61995	52 192	168 1 1	127	172.2	7 5 69		TLSV	1.2	313	ITCP Provious segment not captured]	
17 0.774288 192.168.1.1 192.168.1.127 DNS 106 Standard query exponse 0x4055 A m.qp. 18 0.899443 192.168.1.127 192.168.1.127 DNS 74 Standard query exponse 0x4055 A m.qp. 20 0.93515 192.168.1.127 192.168.1.127 Standard query exponse 0x4055 A m.qp. 20 0.913483 192.168.1.127 66.198.24.243 TCP 74 40356 - 80 [SYN] Seq=8 Win-65535 Len 21 0.948886 192.168.1.127 66.198.24.243 TCP 74 443176 - 443 [SYN] Seq=8 Win-65535 Len 22 0.960731 192.168.1.127 66.198.24.243 TCP 74 443176 - 443 [SYN] Seq=8 Win-65535 Len 23 1.922539 66.198.24.243 192.168.1.127 TCP 74 443176 - 443 [SYN] Seq=8 Win-65535 Len 23 1.922539 66.198.24.243 192.168.1.127 TCP 74 443176 - 443 [SYN] Seq=8 Win-65535 Len 23 1.922539 66.198.24.243 192.168.1.127 TCP 74 44316 - 443 [SYN] Seq=8 Win-65535 Len 24 1.943488 193.11 186.81 192.168.1.27 TCP 74 44316 - 443 [SYN] Seq=8 Win-65535 Len 24 1.943488 193.11 186.81 192.168.1.27 TCP 74 4435 [SYN] Seq=1 Ack=61 Win-29 24 1.943488 198.11 186.81 192.168.1.27		16 0 60507	JU 102. 70 170	217 5 6	127 89	102.1	10 1 127		TCD		88	[TCP ACKed unseen segment] 442 - 4652	
18 0.898443 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x16da A xww.taobao.co 19 0.893515 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x16da A xww.taobao.co 20 0.913483 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x16da A xww.taobao.co 21 0.948806 192.168.1.127 192.168.1.127 192.168.1.127 194.43170 74 43170 443.56 21 0.948806 192.168.1.127 198.11.186.81 TCP 74 443170 443.584.00 105.553.5 Len 21 0.948806 192.168.1.127 192.168.1.127 TCP 74 443170 443.584.00 Seq=9 Win=55535 Len 22 0.960731 192.168.1.127 TCP 74 443.544.00 Seq=1 Ack=61 Win=29 Ack=70 Win=5535 Len 23 1.922539 66.198.24.243 192.168.1.27 TCP 74 443.444.544.544 Seq=1 Ack=61 Win=29 24 1 191488 198.1186.81 192.168.1.27 TCP 74 443.444.544 Seq=1 Ack=61 Win=29 24 1 191488 198.1186.81 192.168.1.27 TCP 74 443.444.544 Seq=1 Ack=61 Win=29 24 1 191488 198.186.23 192.946.1.23 <td></td> <td>17 0.77426</td> <td>18 192</td> <td>168 1 1</td> <td>1</td> <td>192.16</td> <td>18.1.127</td> <td></td> <td>DNS</td> <td></td> <td>168</td> <td>Standard query response 0x4cb5 A m qn</td> <td></td>		17 0.77426	18 192	168 1 1	1	192.16	18.1.127		DNS		168	Standard query response 0x4cb5 A m qn	
19 0.893515 192.168.1.127 192.168.1.1 DNS 64 Standard query 0x4643 AAAA mygw.alipp 28 0.913483 192.168.1.127 66.199.24.243 TCP 74 40356 - 80 [SYN] Seq=0 Win=65535 Len 22 0.966731 192.168.1.127 66.199.24.243 TCP 74 443170 - 443 [SYN] Seq=0 Win=65535 Len 23 1.022539 66.198.24.243 192.168.1.127 66.198.24.243 HTTP 114 HEAD / HTTP/1.1 23 1.022539 66.198.24.243 192.168.1.127 TCP 54 80 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1.91488 198.11.186.81 192.168.1.127 TCP 54 80 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1.91488 198.11 186.81 192.168.1.127 TCP 54 80 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1.91488 198.11 186.81 192.168.1.127 TCP 74 4d35 - 48176 [SVN ArK1 Senm8 Ack=1 Win Frame 4: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) Ethernet II, Src: HuawesTe_B8:3d:23 (80:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:		18 0.89844	13 192	168.1.1	127	192.10	38.1.1		DNS		74	Standard query 9x16da A www.tanhao.co	
20 0.913483 192.168.1.127 66.190.24.243 TCP 74 46356 - 80 [SYN] Seq=0 Win=65355 Len= 21 0.94880 192.168.1.127 198.11.186.81 TCP 74 46376 - 443 [SYN] Seq=0 Win=65355 Len= 21 0.94880 192.168.1.127 198.11.186.81 TCP 74 46376 - 443 [SYN] Seq=0 Win=65355 Len= 21 0.94880 192.168.1.127 198.11.127 TCP 74 46376 - 443 [SYN] Seq=0 Win=65355 Len= 23 1.022539 66.190.24.243 192.168.1.127 TCP 54 00 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1 191488 198.11 186.81 192.168.1.127 TCP 54 00 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1 191488 198.11 186.81 192.168.1.27 TCP 74 4d3 - 43376 [SyN] Ack1 Seq=0 Ack=1 Win=29 24 1 191488 198.11 186.81 192.168.1.27 TCP 74 4d3 - 43376 [SyN] Ack1 Seq=0 Ack=1 Win=29 24 1 191488 198.11 186.81 192.108.1.27 TCP 74 4d3 - 43376 [SyN] Ack1 Seq=0 Ack=1 Win=29 Ethernet II, Src: HuaweIre_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:		19 0.89351	15 192	.168.1.1	127	192.10	38.1.1		DNS		84	Standard query 8x4643 AAAA myow.alipa	
21 0.948800 192.168.1.127 198.11.186.81 TCP 74.431(0) - 443 431(0) - 443 Styl) Seg=8 Win=65535 Len 22 0.960731 192.168.1.127 66.198.24.243 HTTP 114 HEAD / HTTP/1.1 23 1.922539 66.198.24.243 192.168.1.127 TCP 54.80 - 40356 [ACK] Seg=1 Ack=61 Win=29 24 1.94488 194.11 184.84 192.168.1.127 TCP 74.443 - 4374 Seg=8 Ark=61 Win=29 24 1.94488 194.184.81 192.168.1.27 TCP 74.443 - 4374 Seg=8 Ark=61 Win=29 24 1.94488 194.184.81 192.168.1.27 TCP 74.443 - 4374 Seg=8 Ark=61 Win=29 24 1.94488 194.184.81 192.168.1.27 TCP 74.443 - 4374 Seg=8 Ark=61 Win=29 24 1.94488 194.184.81 192.168.1.27 TCP 74.443 - 4374 Seg=8 Ark=61 Win=29 25 25.43 194.184.123 195.168.123 195.168.123 195.168.123 195.168.123 195.14.445.25 195.255.255.255.255 195.255.255.255 195.255.255.255 195.255.255 195.255.255 2600 ff ff ff ff ff ff 60 9a cd b8 3d 23 08 00 45 10 =#-E. 27.052.01 dec cdo Bo		20 0.91348	13 192	.168.1.1	127	66.19	3.24.243		TCP		74	40356 → 80 [SYN] Seq=0 Win=65535 Len=	_
22 0.966731 192.168.1,127 66.198.24.243 HTTP 114 HEAD / HTTP/1.1 23 1.622539 66.198.24.243 192.168.1.127 TCP 54 80 - 40356 [ACK] Seq=1 Ack=61 Win=29 23 1.922539 66.198.24.243 192.168.1.127 TCP 74 443 - 40356 [ACK] Seq=1 Ack=61 Win=29 24 1.9438 194.11 H& R4 192.168.1 127 TCP 74 443 - 43378 [SVN ArK] Seq=8 Ark=1 Win Frame 4: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) Ethernet II, Src: Huawe3Te_b8:3d:23 (80:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:		21 0.94886	10 192	.168.1.1	127	198.1	1.186.81		TCP		74	43170 → 443 [SYN] Seg=0 Win=65535 Len	
23 1.022539 66.196.24.243 192.168.1.127 TCP 54 80 - 40356 fACK Seq=1 Ack=61 Win=29 24 1 191488 198.11 186.81 192.168.1.127 TCP 74 433 - 43178 fSVN Ack1 Seq=1 Ack-61 Win=29 Frame 4: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) Ethernet 11, Src: HuaweiTe_b8:3d:23 (80:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	_	22 0,96673	31 192	.168.1.1	127	66.19	3.24.243	_	HTTP		114	HEAD / HTTP/1.1	
241 191 192 188 192 158 192 158 192 158 192 158 192 158 192 158 192 158 192 158 192 158 192 158 192 158 192 158 <th167< th=""> <th167< th=""> <th167< th=""></th167<></th167<></th167<>		23 1.02253	19 66.	198.24.2	243	192.10	38.1.127		TCP		54	80 → 40356 [ACK] Seg=1 Ack=61 Win=29	_
Frame 4: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) Ethernet II, Src: HuaweJie_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:		24 1.19148	198	11 186	81	192.16	58.1.127		TCP		74	443 → 43170 [SYN ACK] Sec=0 Ack=1 Wi	
000 ff ff ff ff ff ff ff 60 9a cd b8 3d 23 88 60 45 10	FI Et II Us Bo	ame 4: 368 b hernet II, S ternet Proto er Datagram otstrap Prof	bytes on wi Src: Huawei ocol Versio Protocol, S tocol (Requ	re (2944 Te_b8:30 n 4, Src Src Port est)	4 bits), d:23 (00 c: 0.0.0 t: 68, D	368 byt :9a:cd:b .0, Dst: st Port:	es captun 8:3d:23), 255.255. 67	red (2 , Dst: .255.2	2944 bi : Broad 255	ts) cast	t (ff:1	ff:ff:ff:ff:ff)	
Dackate: 1669, Dicelayed: 1669 (100,094) Depfile: Defa	300	9 TT TT TT	TT TT II 00	9 9a cd	1 D8 3d 2	3 88 00	45 10			=# · ·	E.		
USAR (MS-11) - DEC CRD USAR (1001 108)			1 de									Instant COR Displayed 1000 (100 00() Destiles D	

- MD5 for jdyco001 is d7c49808446d3257c2ecbd70beb7271e so I used WPA2-P5-01.cap
- I used aircrack-ng to open the file
- There was only 1 option so I selected it
- I copied rockyou.txt.gz to desktop where I moved the .cap file
- I used aircrack to find the WPA key.
- I used the airdecap to create the decap file and review the traffic
- In my analysis, I noticed that IPV4 has majority of the protocols with 99.4%, UDP at 55.5%, TCP at 41.9% an TCP at 43.8% of all data packets.