Network And Device Forensic Analysis Of Android Social-Messaging Applications

By

Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Frank Breitinger and Jason Moore

Presented At

The Digital Forensic Research Conference

DFRWS 2015 USA Philadelphia, PA (Aug 9th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Network and device forensic analysis of Android social-messaging applications

Daniel Walnycky, Ibrahim Baggili, Andrew Marrington,
Jason Moore, Frank Breitinger

Graduate Research Assistant, UNHcFREG Member
Presenting @ DFRWS, Philadelphia, PA, 2015

University *of* New Haven

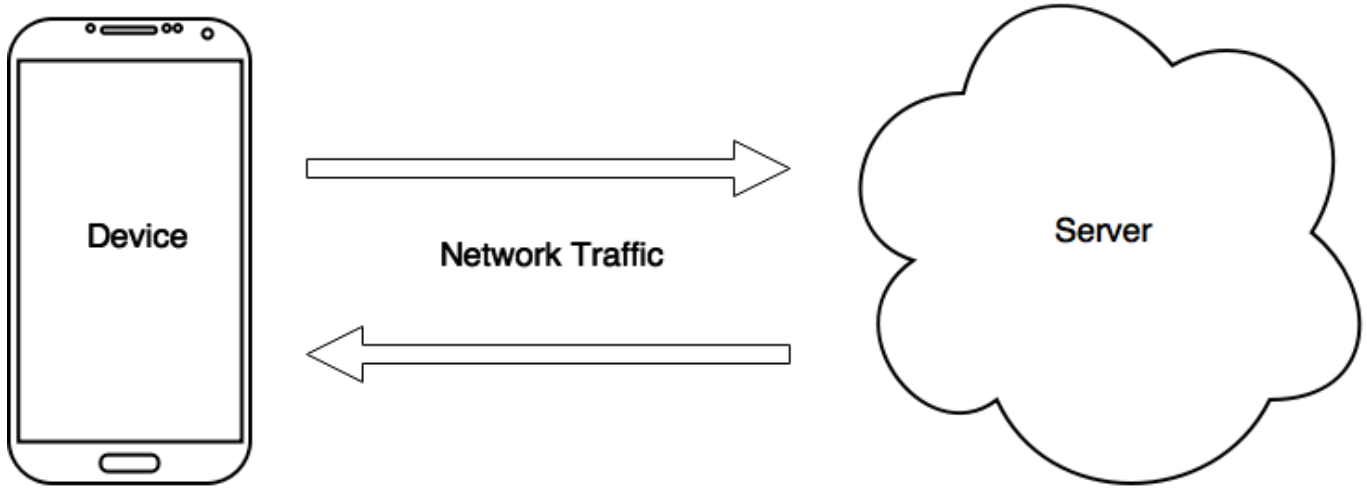
Agenda

- Introduction
- Related work
- Methodology
- Experimental results
- Discussion and conclusion
- Future work
- Datapp

Introduction

Tested 20 Android messaging apps for “low hanging fruit” a.k.a unencrypted data:

- on the device, in network traffic, and on server storage



Found evidentiary traces: passwords, screen shots, text, images, videos, audio, GPS location, sketches, profile pictures, and more…

Related work

- Forensic value of smartphone messages:
  - Smartphones may contain the same rich variety of digital evidence which might be found on a computer system (Lessard & Kessler, 2010)
  - Smartphones and their applications may be involved in a huge variety of criminal cases (Taylor et al., 2012)

- Smartphone application forensics:
  - As instant messenger programs for PC were ported over to smartphones the forensic community followed (Husain & Sridhar, 2010); (Al Mutawa et al., 2012)
  - WhatsApp device storage analysis reconstructed contact lists and chat logs (Anglano, 2014)

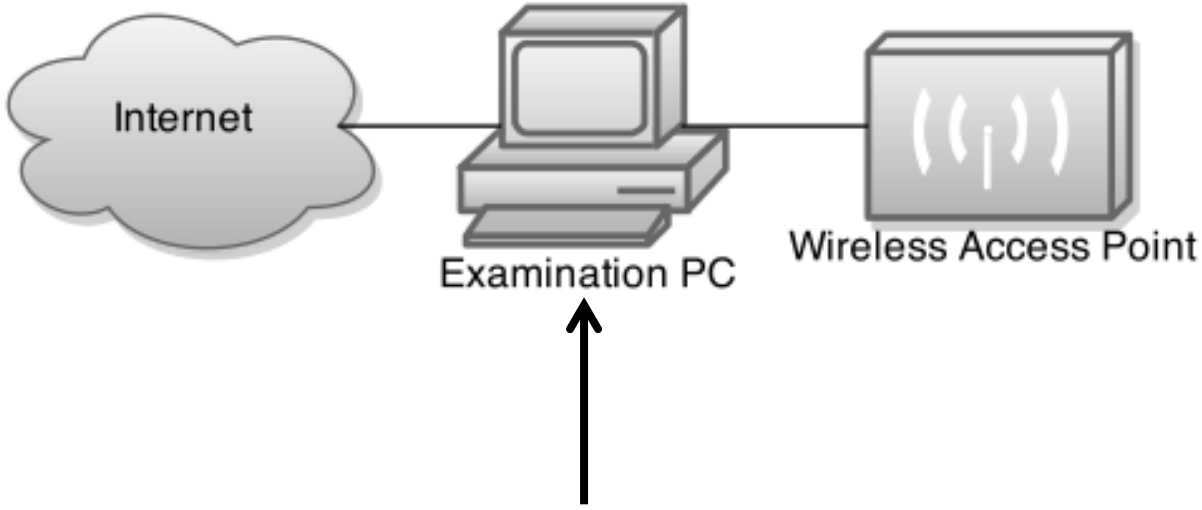
Related work cont.

- Apps being targeted for cyber attacks:
  - 1414 vulnerabilities found in top 50 paid and top 50 free Android apps (Chin et al., 2011)
  - Vulnerabilities to account hijacking, spoofing, and other attack vectors found on 9 popular messaging apps for Android (Schrittwieser et al., 2012)

Methodology

- 20 messaging apps from Google Play store based on:
  - Search terms
  - Number of downloads
- Focused on *person to person* communication
  - Ex. Instagram Direct Feature
  - Users think it's "private"
- Signed up for services using the devices prior to data collection

Network traffic analysis experimental setup



MiTM:

All traffic to and from the Android device is passing through our laptop

Network traffic analysis experimental setup

STEP 1: Connect the hosted computer to the internet via Ethernet

STEP 2: The Ethernet connection was set to share it's internet access with the virtual WiFi mini port adapter

STEP 3: Virtual network was setup with the command:

- *"netsh wlan set hostednetwork mode=allow ssid=test key=1234567890"*

STEP 4: The virtual network was enabled with the command:

- "*netsh wlan start hostednetwork*"

STEP 5: We connected to the "test" network from our target HTC one

A video demonstration of this process can be viewed at www.youtube.com/unhcfreg

Network traffic analysis experimental setup

Network traffic analysis tools:

Device/Tool	Use	Software/OS Version
Laptop	Create test network using virtual mini port adapter	Windows 7 SP2
One M8 (UNHcFREGdroid)	Connected to test network	Android 4.4.2
IPad 2 (UNHcFREGapple)	Connected outside test network	iOS 7.1.2
NetworkMiner	Observe live network traffic	1.6.1
Wireshark	Record live network traffic to pcap file for each app	1.10.8
NetWitness Investigator	Verify findings/post-analysis from pcap files	9.7.5.9

Network traffic evidence types:

Text messages, images, video, audio, GPS location, sketches, and more

Device storage analysis experimental setup

Device storage analysis tools:

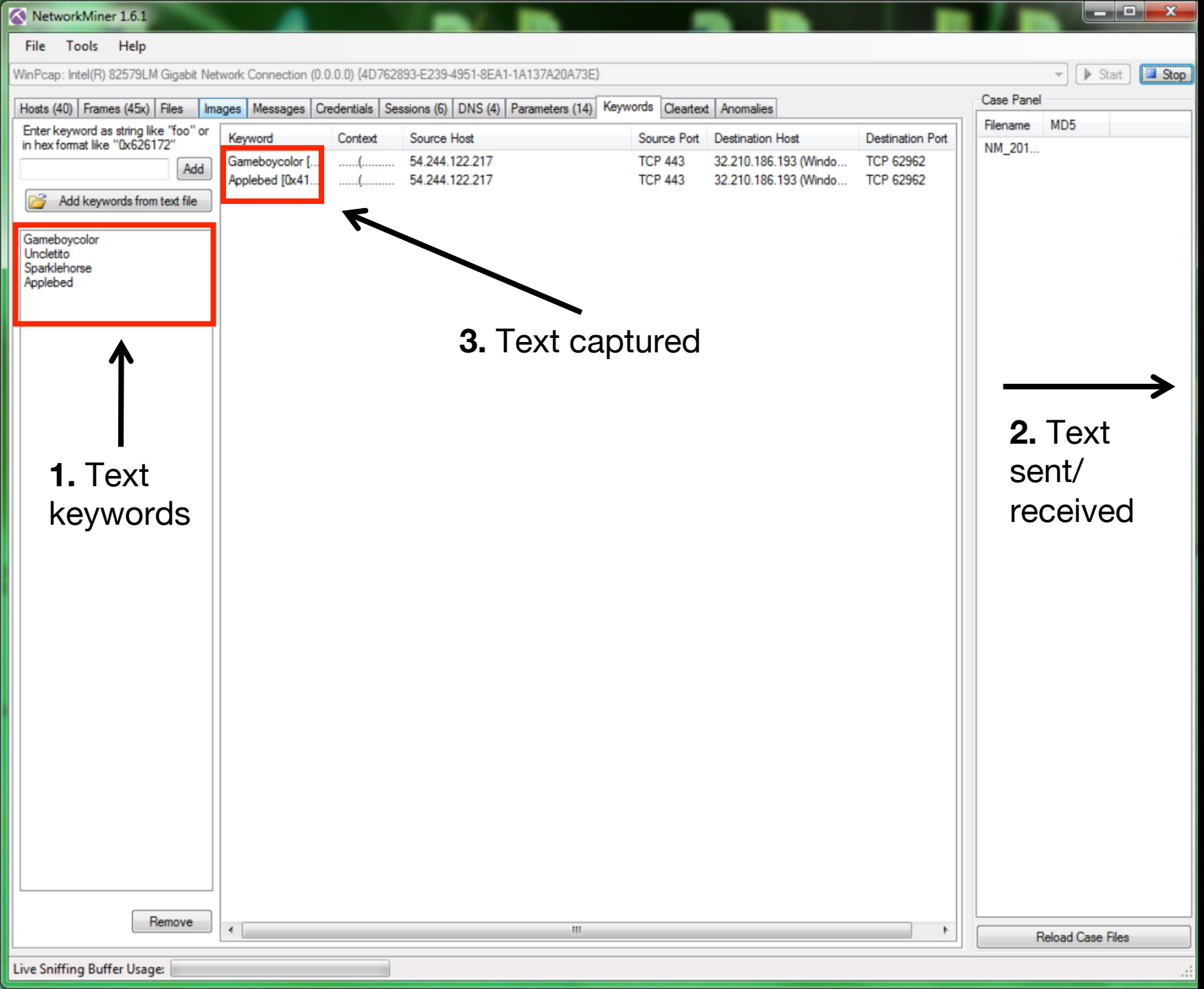
Device/Tool	Use	Software/OS Version
Laptop	Running analysis software	Windows 7 SP2
One M8 (UNHcFREGdroid)	Connected to PC through USB	Android 4.4.2
XRY	Logical image creator/viewer	6.10.1
Helium Backup	Verify findings/create Android backup	1.1.2.1
Android Backup Extractor	View Android backup	2014-06-30
SQLite Database Browser	View Sqlite/DB files	3.2.0

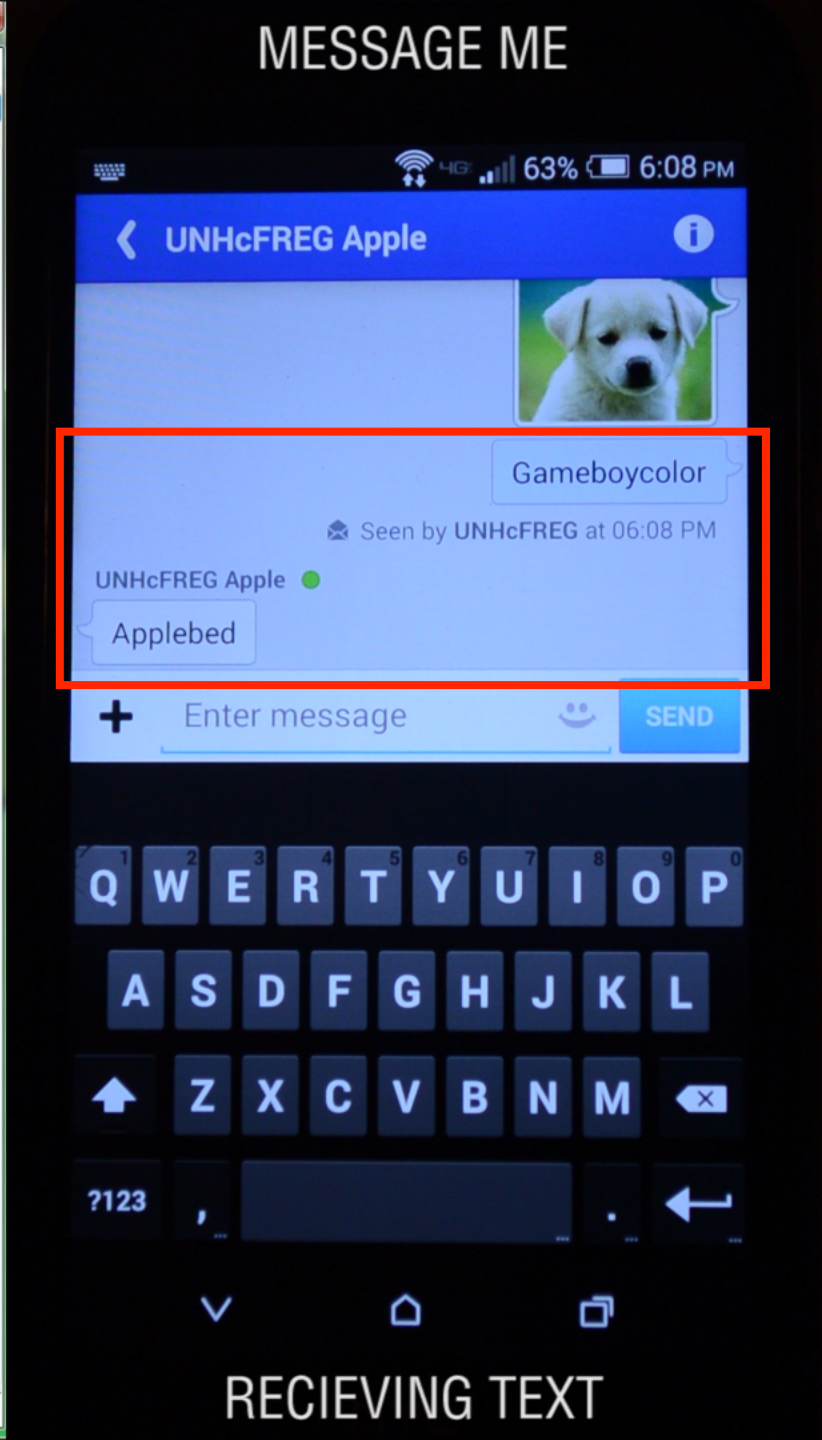
Device storage evidence types:

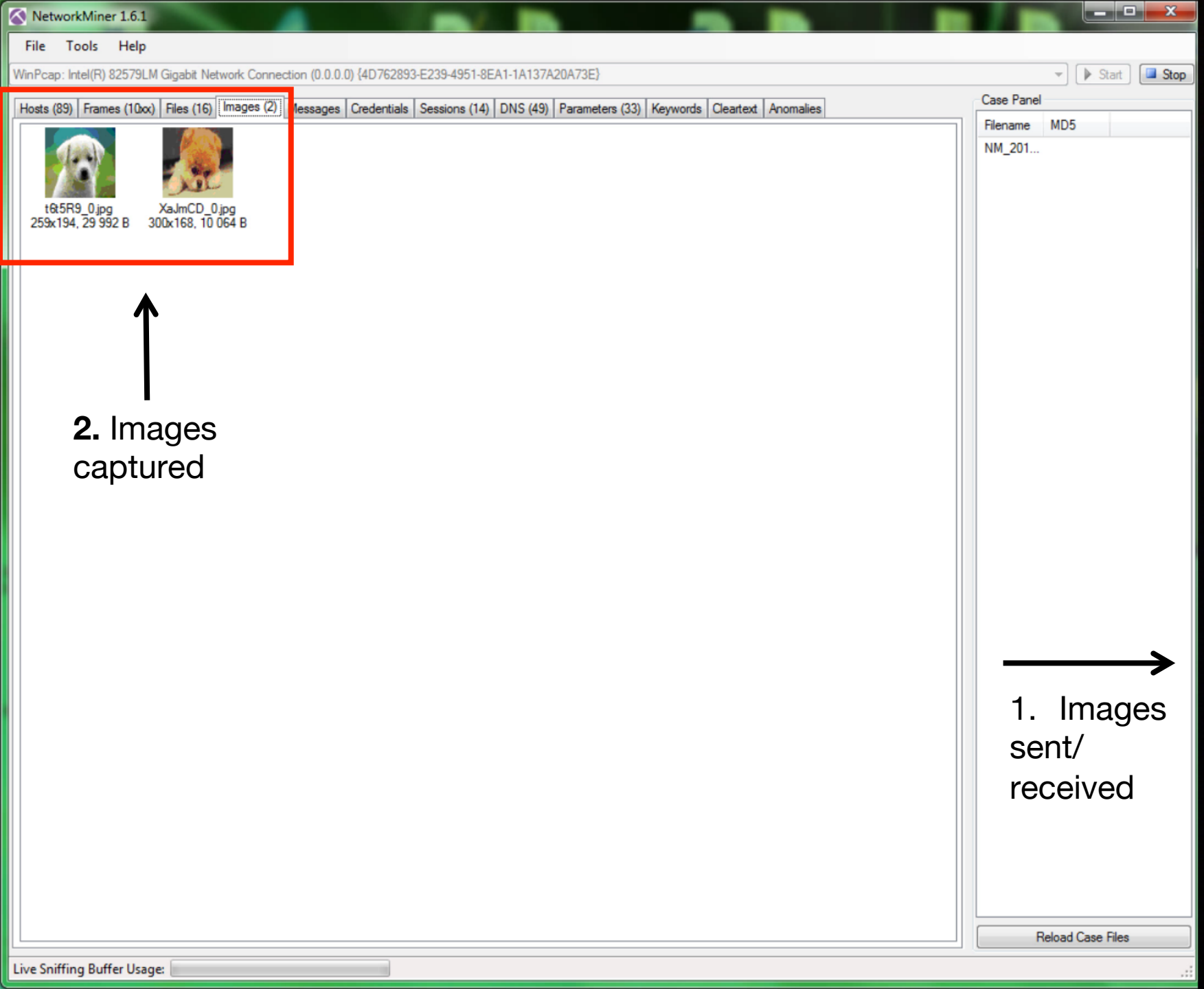
Chat logs and user credentials within DB files

Experimental results overview

- Network traffic evidence acquisition
- Device storage evidence acquisition
- Encrypted apps
- Summary of all evidence recovered

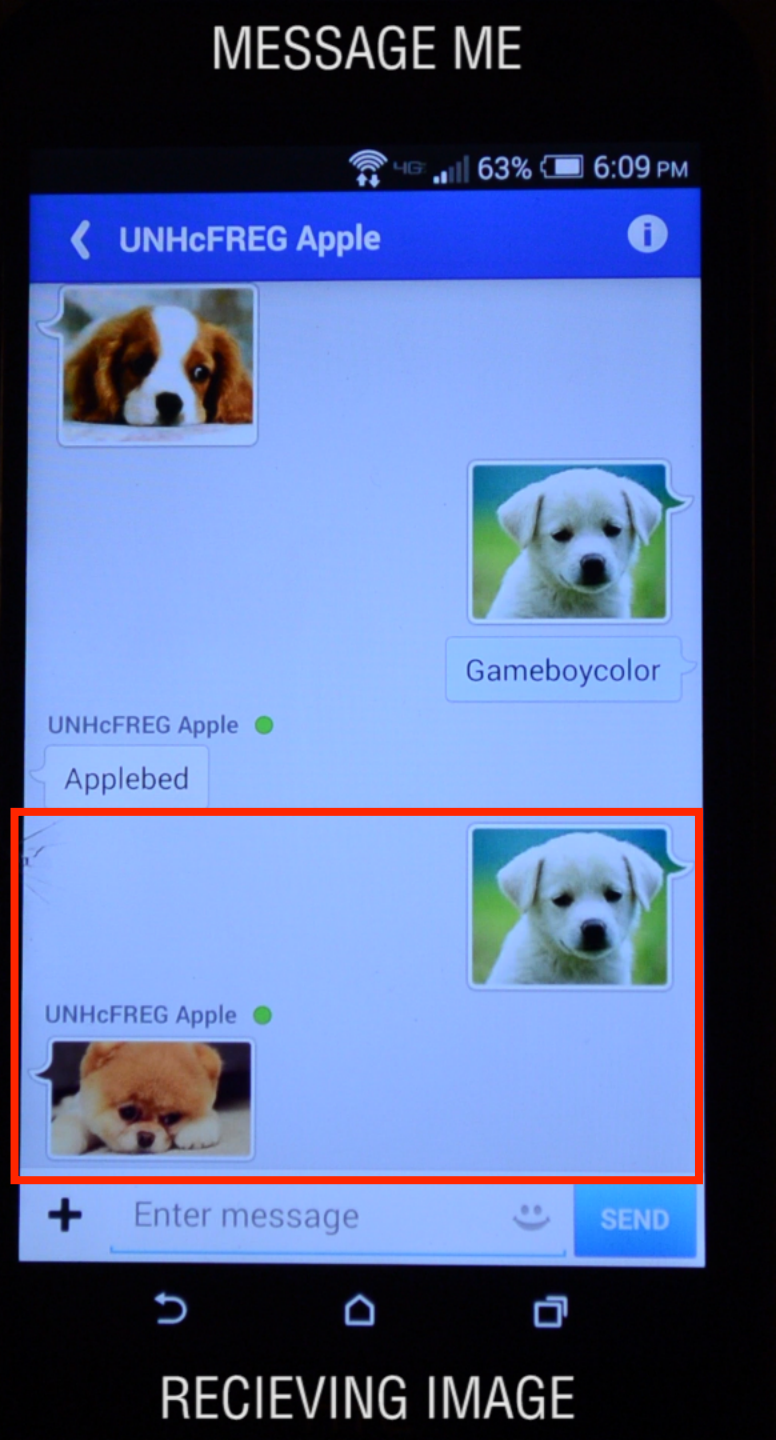

NetworkMiner 1.6.1
File Tools Help
WinPcap: Intel(R) 82579LM Gigabit Network Connection (0.0.0.0) {4D762893-E239-4951-8EA1-1A137A20A73E}
Start
Stop
Hosts (40) Frames (45x) Files Images Messages Credentials Sessions (6) DNS (4) Parameters (14) Keywords Cleartext Anomalies
Enter keyword as string like "foo" or in hex format like "0x626172"
Add
Add keywords from text file
Gameboycolor
Uncletito
Sparklehorse
Applebed
Remove
Keyword Context Source Host Source Port Destination Host Destination Port
Gameboycolor [... .....(..... 54.244.122.217 TCP 443 32.210.186.193 (Windo... TCP 62962
Applebed [0x41... .....(..... 54.244.122.217 TCP 443 32.210.186.193 (Windo... TCP 62962
Case Panel
Filename MD5
NM_201...
Reload Case Files
Live Sniffing Buffer Usage:
1. Text keywords
3. Text captured
2. Text sent/ received

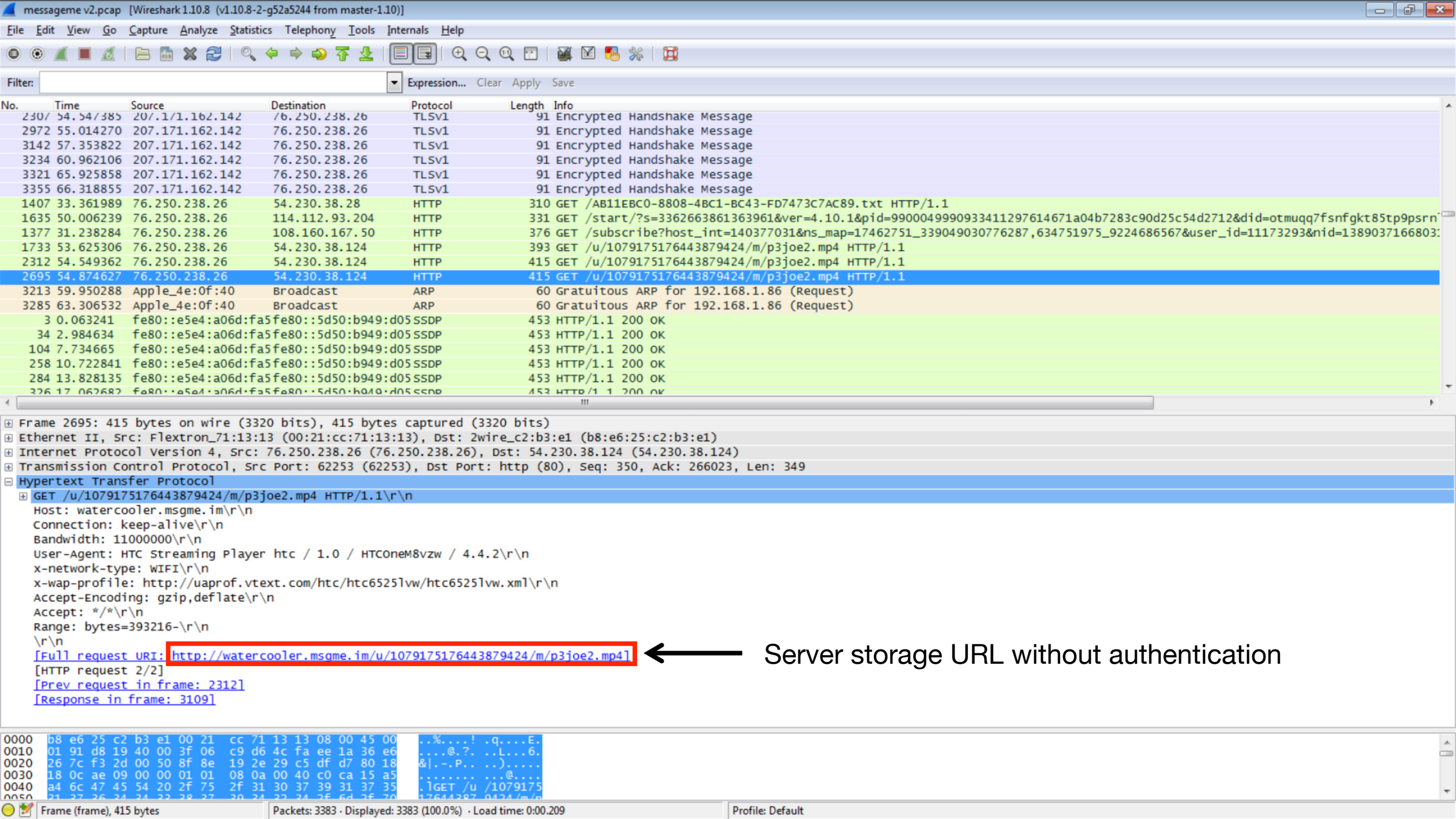

MESSAGE ME
63% 6:08 PM
UNHcFREG Apple
Gameboycolor
Seen by UNHcFREG at 06:08 PM
UNHcFREG Apple
Applebed
Enter message
SEND
RECIEVING TEXT



2. Images captured

1. Images sent/ received




messageme v2.pcap [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2307 54.547385 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
2972 55.014270 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
3142 57.353822 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
3234 60.962106 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
3321 65.925858 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
3355 66.318855 207.171.162.142 76.250.238.26 TLSv1 91 Encrypted Handshake Message
1407 33.361989 76.250.238.26 54.230.38.28 HTTP 310 GET /AB11EBC0-8808-4BC1-BC43-FD7473C7AC89.txt HTTP/1.1
1635 50.006239 76.250.238.26 114.112.93.204 HTTP 331 GET /start/?s=3362663861363961&ver=4.10.1&pid=990004999093341129761467 1a04b7283c90d25c54d2712&did=otmuqq7fsnfgkt85tp9psrn
1377 31.238284 76.250.238.26 108.160.167.50 HTTP 376 GET /subscribe?host_int=140377031&ns_map=17462751_339049030776287,634751975_9224686567&user_id=11173293&nid=1389037166803
1733 53.625306 76.250.238.26 54.230.38.124 HTTP 393 GET /u/1079175176443879424/m/p3joe2.mp4 HTTP/1.1
2312 54.549362 76.250.238.26 54.230.38.124 HTTP 415 GET /u/1079175176443879424/m/p3joe2.mp4 HTTP/1.1
2695 54.874627 76.250.238.26 54.230.38.124 HTTP 415 GET /u/1079175176443879424/m/p3joe2.mp4 HTTP/1.1
3213 59.950288 Apple_4e:0f:40 Broadcast ARP 60 Gratuitous ARP for 192.168.1.86 (Request)
3285 63.306532 Apple_4e:0f:40 Broadcast ARP 60 Gratuitous ARP for 192.168.1.86 (Request)
3 0.063241 fe80::e5e4:a06d:fa5 fe80::5d50:b949:d05 SSDP 453 HTTP/1.1 200 OK
34 2.984634 fe80::e5e4:a06d:fa5 fe80::5d50:b949:d05 SSDP 453 HTTP/1.1 200 OK
104 7.734665 fe80::e5e4:a06d:fa5 fe80::5d50:b949:d05 SSDP 453 HTTP/1.1 200 OK
258 10.722841 fe80::e5e4:a06d:fa5 fe80::5d50:b949:d05 SSDP 453 HTTP/1.1 200 OK
284 13.828135 fe80::e5e4:a06d:fa5 fe80::5d50:b949:d05 SSDP 453 HTTP/1.1 200 OK
Frame 2695: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits)
Ethernet II, Src: Flextron_71:13:13 (00:21:cc:71:13:13), Dst: 2wire_c2:b3:e1 (b8:e6:25:c2:b3:e1)
Internet Protocol Version 4, Src: 76.250.238.26 (76.250.238.26), Dst: 54.230.38.124 (54.230.38.124)
Transmission Control Protocol, Src Port: 62253 (62253), Dst Port: http (80), Seq: 350, Ack: 266023, Len: 349
Hypertext Transfer Protocol
GET /u/1079175176443879424/m/p3joe2.mp4 HTTP/1.1\r\n
Host: watercooler.msgme.im\r\n
Connection: keep-alive\r\n
Bandwidth: 11000000\r\n
User-Agent: HTC Streaming Player htc / 1.0 / HTCOneM8vzw / 4.4.2\r\n
x-network-type: WIFI\r\n
x-wap-profile: http://uaprof.vtext.com/htc/htc6525lvw/htc6525lvw.xml\r\n
Accept-Encoding: gzip,deflate\r\n
Accept: */*\r\n
Range: bytes=393216-\r\n
\r\n
[Full request URI: http://watercooler.msgme.im/u/1079175176443879424/m/p3joe2.mp4]
[HTTP request 2/2]
[Prev request in frame: 2312]
[Response in frame: 3109]
Server storage URL without authentication
0000 b8 e6 25 c2 b3 e1 00 21 cc 71 13 13 08 00 45 00
0010 01 91 d8 19 40 00 3f 06 c9 d6 4c fa ee 1a 36 e6
0020 26 7c f3 2d 00 50 8f 8e 19 2e 29 c5 df d7 80 18
0030 18 0c ae 09 00 00 01 01 08 0a 00 40 c0 ca 15 a5
0040 a4 6c 47 45 54 20 2f 75 2f 31 30 37 39 31 37 35
Frame (frame), 415 bytes
Packets: 3383 · Displayed: 3383 (100.0%) · Load time: 0:00.209
Profile: Default

9 of 20 apps tested had unencrypted user files on application servers

5 of these 9 links still work today

Unencrypted user files on application servers

Application	URL for Server-side Media
Viber	https://s3.amazonaws.com/share2014-04-21/0d1b42b9f6be43c8b83f0ea4b141f8fae4fb5d775093a17c0e06861c6e2e9300.mp4
Instagram	http://photos-e.ak.instagram.com/hphotos-ak-xaf1/10553994_908375655855764_354550189_n.jpg
ooVoo	http://g-ugc.oovoo.com/nemo-ugc/40051d186b955a77_b.jpg
Tango	http://cget.tango.me/contentserver/download/U8gkjgAAvvzybrAuOcfZPw/9b4IqEqk
MessageMe	http://watercooler.msgme.im/u/10791751764438794 24/m/p3joe2.mp4
Grindr	http://cdns.grindr.com/grindr/chat/aa0e6063299350a9b80278feb56a8606acae1267
HeyWire	http://mms.heywire.com/cs/GetImage.aspx?c=p-&p=0%2fmms1%2f20140725%2fp-ec2f6715-afeb-4db4-a5c0-8aaf8ac80689.jpeg
TextPlus	https://d17ogcqyct0vcy.cloudfront.net/377/549/1Kw7ihM5Ri1OkDoXWa.jpg
Facebook Messenger	http://scontent-lga.xx.fbcdn.net/hphotos-xpf1/v/t34.0-12/11156748_10152706456535706_749142264_n.jpg?oh=efbf52c9c9f74525ced5d3d17642ae69&oe=553AE540

Working links to user files on app servers

textPlus: https://d17ogcqyct0vcy.cloudfront.net/377/549/1Kw7ihM5Ri1OkDoXWa.jpg

Oovoo: http://g-ugc.oovoo.com/nemo-ugc/40051d186b955a77_b.jpg

Instagram: http://photos-e.ak.instagram.com/hphotos-ak-xaf1/10553994_908375655855764_354550189_n.jpg

Tango: http://cget.tango.me/contentserver/download/U8gkjgAAvvzybrAuOcfZPw/9b4IqEqk

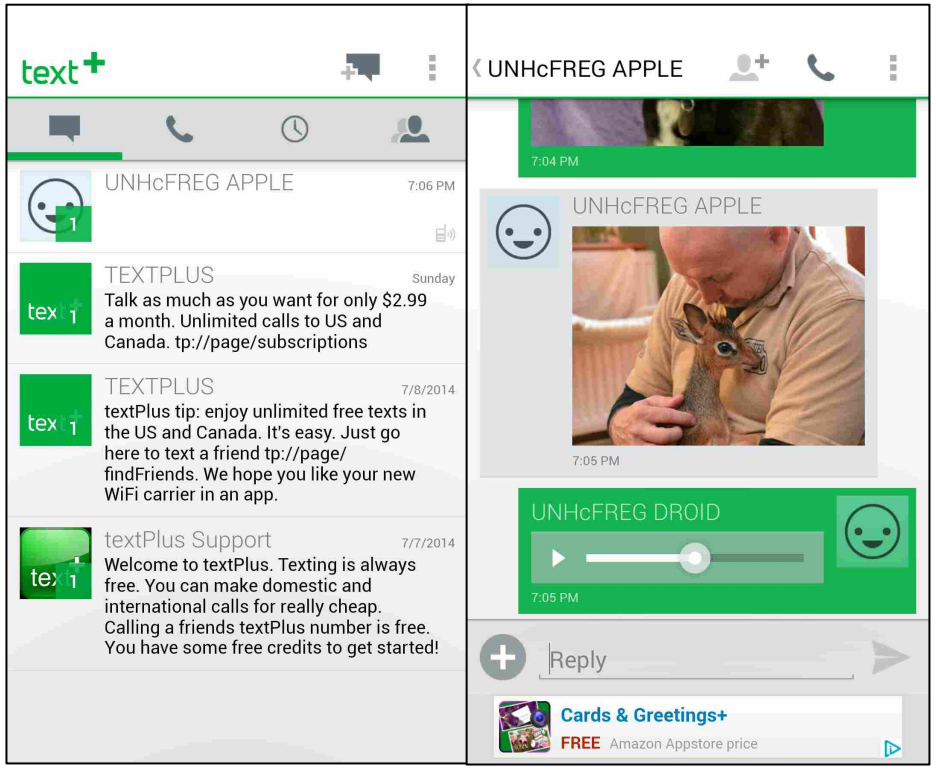
Grindr: http://cdns.grindr.com/grindr/chat/aa0e6063299350a9b80278feb56a8606acae1267

	id	key	value
	Filter	Filter	Filter
1	24	database.migration	3
2	47	user.username	unhcfregdroid
3	48	user.email	[redacted]@live.com
4	49	user.phone	+1203[redacted]
5	50	user.sms_number	+1914[redacted]
6	51	user.gender	m
7	52	user.birthday	1992/07/22
8	53	user.password	gin[redacted]
9	54	user.password_hashed	false
10	55	user.userId	47763570

TextMe's “database.sql” with user data in plaintext

8 of 20 apps tested had at least unencrypted chat logs in DB files

- TextMe and Nimbuzz had passwords in plain text
- textPlus took and stored screenshots of user activity



Unencrypted chat logs/user credentials in App DB files

Application	Location of user data on Android device
textPlus	com.gogii.textplus.ab/textPlus.db
Nimbuzz	com.nimbuzz.ab/Nimbuzz.db
TextMe	com.textmeinc.textme.ab/Database.sql
MeetMe	com.myyearbook.m.ab/Chats.db
Kik	kik.android.ab/kikDatabase.db
ooVoo	com.oovoo.ab/Core.db
HeyWire	com.mediafriends.chime.ab/HWProvider.db
Hike	com.bsb.hike.ab/chats.db

Experimental results

Applications tested with no evidence recovered

Applications	Capabilities	Performed Activity	Encrypted Network Traffic, Data Storage, and Server Storage	Emphasized Security
Tinder	Text	Sent/Received text	Yes	No
Wickr	Text and image sharing	Sent/Received text Sent/Received image	Yes	Yes
Snapchat	Text, image, and video sharing	Sent/Received text Sent/Received image Sent/Received video	Yes	No
BBM	Text and image sharing	Sent/Received text Sent/Received image	Yes	No

Only app to mention security as a feature

- Encryption in network traffic = HTTPS/SSL
- Encryption in data storage = Obfuscated database content

Apps tested/activity performed in order listed → Evidence recovered →

Applications	Capabilities	Performed Activity	Network Traffic Traces	Server Traces	Data Storage Traces
WhatsApp (2.11)	Text, image, video, audio, location, and contact card sharing	Sent/received text Sent/received image Sent/received video Sent/received audio Sent/received GPS location Sent contact card	Contact card (sent), location (sent)		
Viber (4.3.0.712)	Text, image, video, audio, sketch, and location sharing + voice calling	Sent/received text Sent/received image Sent/received video Sent/received audio Sent/received sketch Sent/received GPS location Received voice call	Images (received), video (received), sketches (received), location (sent/received)	Images, video, sketches	
Instagram (6.3.1)	Image and video sharing	Sent/received image Sent/received video	Images (sent/received)	Images	
Okcupid (3.4.6)	Text and image sharing	Sent/received text Sent/received image	Text (sent)		
ooVoo (2.2.1)	Text, image, and video sharing + voice/video calling	Sent/received text Sent/received image Sent/received video	Text (sent/received), images (sent/received)	Images	Chat log
Tango (3.8.95706)	Text, image, video, and audio sharing + voice/video call	Sent/received text Sent/received image Sent/received video Sent/received audio	Images (sent/received), video (sent)	Videos	
Kik (7.3.0)	Text, image, video, and sketch sharing	Sent/received text Sent/received image Sent/received video Sent/received sketch	Sketches (sent)		Chat log
Nimbuzz (3.1.1)	Text, image, video, audio, and location sharing + voice calling	Sent/received text Sent/received image Sent/received GPS location Sent/received video Sent/received audio	Images (sent/received), location (sent), video (sent)		Plain text password, chat log

MeetMe (8.6.1)	Text and image sharing	Sent/received text Sent/received image	Text (sent/received)		Chat log
MessageMe (1.7.3)	Text, image, video, audio, sketch, and location sharing	Sent/received text Sent/received image Sent/received sketch Sent/received GPS location Sent/received video Sent/received audio	Text (sent/received), images (sent/received), sketches (received), location (sent/received), video (sent), audio (sent)	Videos	
TextMe (2.5.2)	Text, image, video, location, and file sharing + voice/video calling	Sent/received text Sent/received image Sent Dropbox file Sent/received video Sent/received GPS location	Images (received), location (sent/received)		Plain text password, chat log
Grindr (2.1.1)	Text, image, and location sharing	Sent/received text Sent/received image Sent/received GPS location	Images (sent)	Images	
HeyWire (4.5.10)	Text, image, audio, and location sharing + voice calling	Sent/received text Sent/received image Sent/received GPS location Sent/received audio	Images (received), location (sent)	Images	Chat log
Hike (3.1.0)	Text, image, video, audio, location, and V-Card sharing + voice calling	Sent/received text Sent/received image Sent/received GPS location Sent/received video Sent/received audio Sent contact card	Location (sent)		Chat log
textPlus (5.9.8)	Text, image, and audio sharing + voice calling	Sent/received text Sent/received image Sent/received audio	Images (sent/received)	Images	App taken screenshot, chat log
Facebook Messenger (25.0.0.17.14)	Text, image, video, audio, location, and stickers sharing + voice calling	Sent/received text Sent/received image Sent/received video Sent/received audio Sent/received GPS location Sent/received stickers	Images (sent/received), video thumbnails (received)	Images, video thumbnails	

A video demonstration of these findings can be viewed at www.youtube.com/unhcfreg

Discussion

- Impact of findings:
  - With access to an app user's phone, passwords are potentially obtainable with db files.
  - With users connected to a rogue access point, large volumes of user data can be captured by an actor.

- App developers were notified of all security issues found:
  - No one responded at first ☹
  - Some responded when we released our results publically

Conclusion

- A lot of these applications are still unsecure, and it's 2015

- This research was done from a forensics perspective, but it opens the door to privacy issues.

Users should: Connect to trusted networks + update and test apps

Investigators should: Explore the potential of network forensics for evidence acquisition

Future Work

- Analyze calling features/undocumented network protocols
  - Karpíšek, Baggili, and Breitinger's WhatsApp call protocol analysis
- Use advanced forensic techniques to pull more data
  - Such as… SSL interception, binary checking, and memory analysis

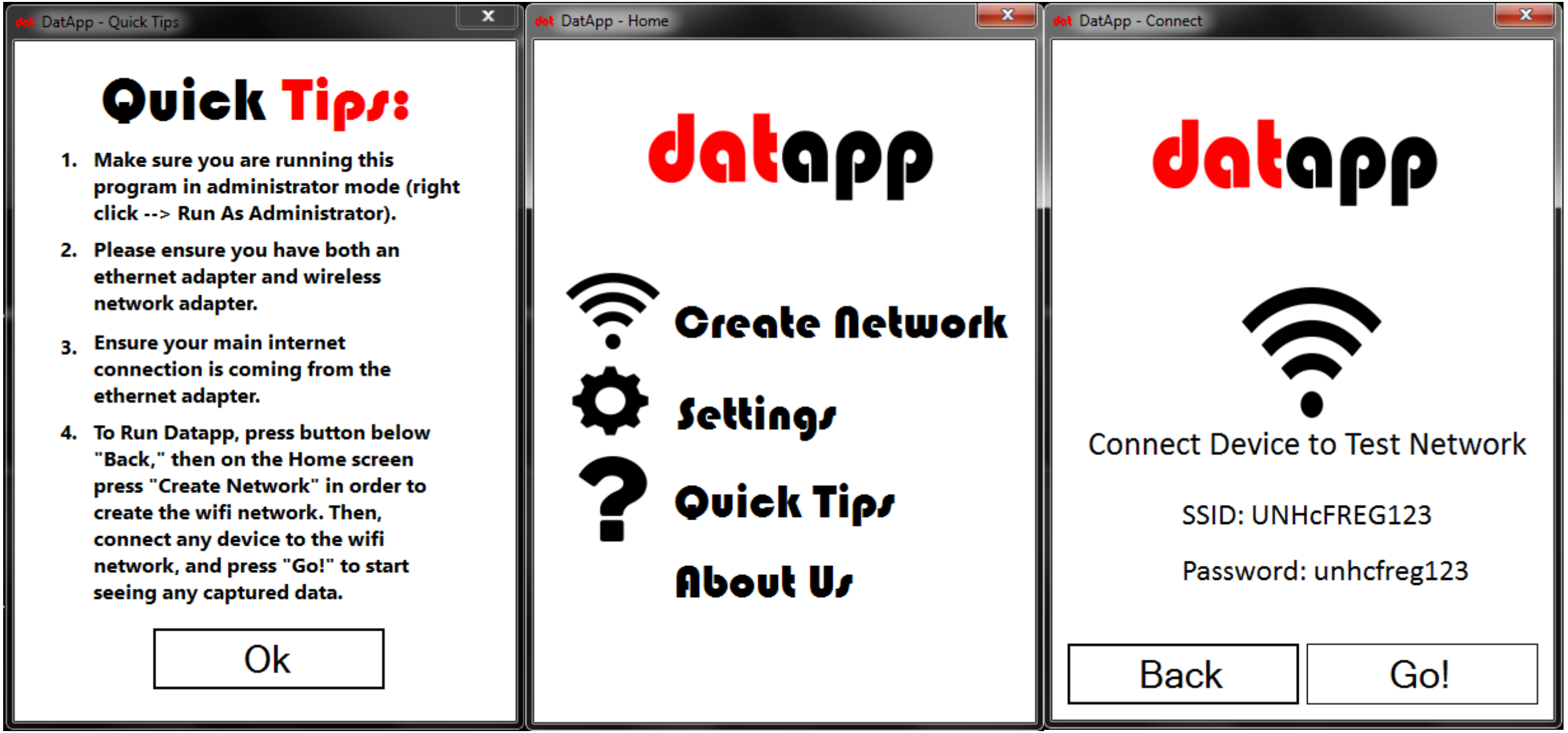
Expand research into more apps for Android, iOS, and other platforms AND continuously test applications as they are updated

- *Cough*Cough* DatApp

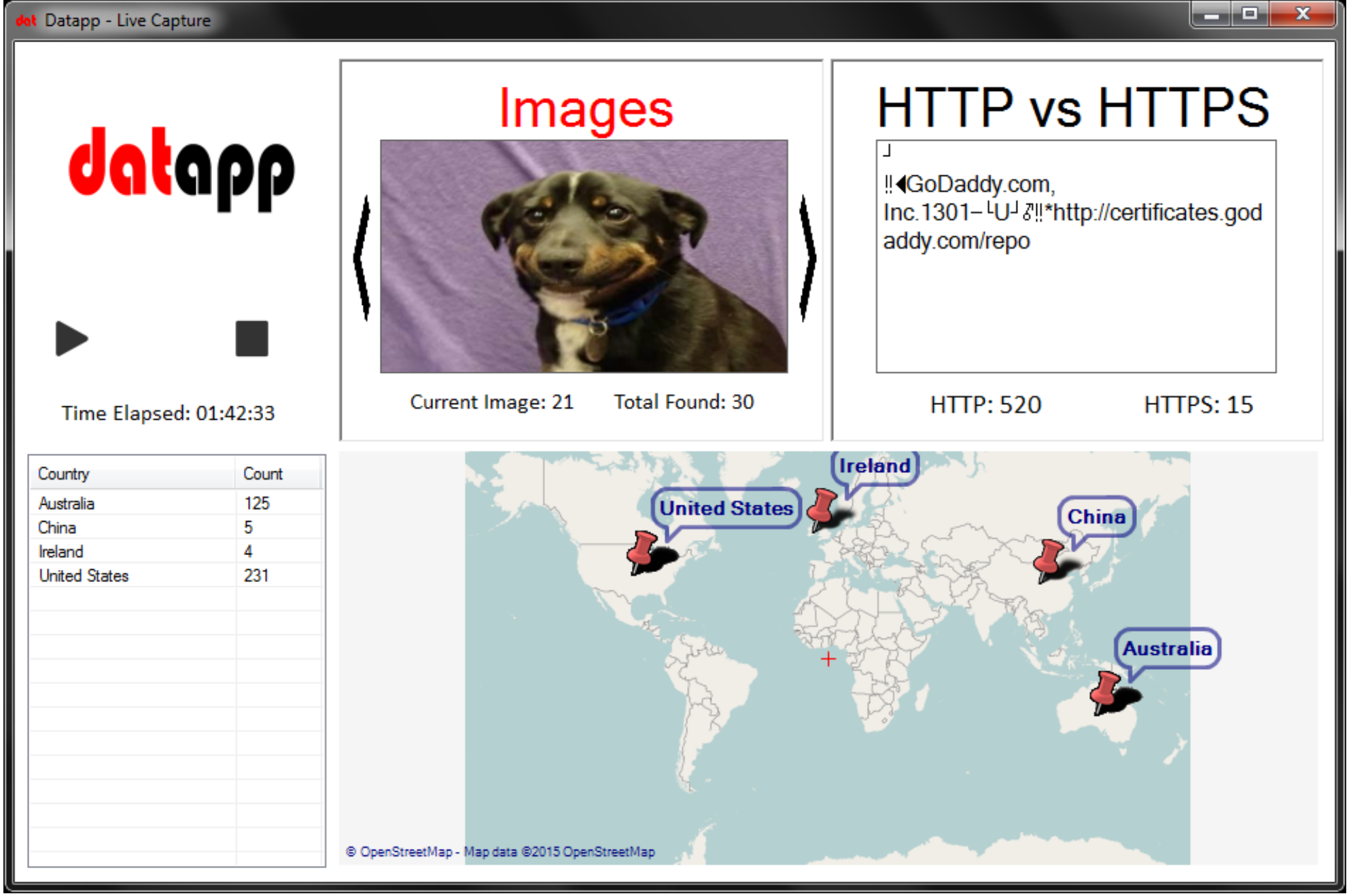
1

2

3



Created by UNHcFREG researchers Roberto Meija and Kyle Anthony.



Datapp is available for download from our website (www.unhcfreg.com) under Data & Tools.

[1] *Ashby v Commonwealth of Australia (No 4) [2012] FCA 1411*

[2] *S v Oscar Pistorius (CC113/2013) [2014] ZAGPPHC 793 (12 September 2014)*

[3] J. Lessard and G. C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations," *Small Scale Digit. Device Forensics J.*, vol. 4, no. 1, 2010.

[4] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, and P. Almond, "Digital evidence from mobile telephone applications," *Comput. Law Secur. Rev.*, vol. 28, no. 3, pp. 335–339, 2012.

[5] S. Y. Willassen, "Forensics and the GSM mobile telephone system," *Int. J. Digit. Evid.*, vol. 2, no. 1, 2003.

[6] M. Husain and R. Sridhar, "iForensics: forensic analysis of instant messaging on smart phones," *Digit. forensics cyber crime*, vol. 31, pp. 9–18, 2010.

[7] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A critical review of 7 years of Mobile Device Forensics," *Digit. Investig.*, vol. 10, no. 4, pp. 323–349, 2013.

[8] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," *Digit. Investig.*, vol. 8, pp. S14–S24, Aug. 2011.

[9] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digit. Investig.*, vol. 9, pp. S24–S33, Aug. 2012.

[10] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," in *Digital Investigation*, 2013, vol. 10, pp. S12–S20.

[11] J. Reust, "Case study: AOL instant messenger trace evidence," *Digit. Investig.*, vol. 3, no. 4, pp. 238–243, 2006.

[12] M. Dickson, "An examination into AOL Instant Messenger 5.5 contact identification," *Digit. Investig.*, vol. 3, no. 4, pp. 227–237, 2006.

[13] M. Dickson, "An examination into Yahoo Messenger 7.0 contact identification," *Digit. Investig.*, vol. 3, no. 3, pp. 159–165, 2006.

[14] M. Dickson, "An examination into MSN Messenger 7.5 contact identification," *Digit. Investig.*, vol. 3, no. 2, pp. 79–83, 2006.

[15] M. Dickson, "An examination into Trillian basic 3.x contact identification," *Digit. Investig.*, vol. 4, no. 1, pp. 36–45, 2007.

[16] M. Kiley, S. Dankner, and M. Rogers, "Forensic Analysis of Volatile Instant Messaging," in *Advances in Digital Forensics IV*, vol. 285, Boston: Springer, 2008, pp. 129–138.

[17] N. Al Mutawa, I. Al Awadhi, I. Baggili, and A. Marrington, "Forensic artifacts of Facebook's instant messaging service," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, 2011, pp. 771–776.

[18] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digit. Investig.*, vol. 11, no. 3, pp. 1–13, 2014.

[19] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. H. Park, "User privacy and modern mobile services: Are they on the same path?," *Pers. Ubiquitous Comput.*, vol. 17, pp. 1437–1448, 2013.

[20] E. Chin, A. Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in Android," *Proc. 9th ...*, pp. 239–252, 2011.

[21] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. Weippl, "Guess who's texting you? evaluating the security of smartphone messaging applications," *Proc. 19th Annu. Symp. Netw. Distrib. Syst. Secur.*, p. 9, 2012.

Contact

dwaln1@unh.newhaven.edu

www.unhcfreg.com

@danwalnycky


Insta
meet me
okc
kik