Ad Evaluation Report

by

Dr. Neal Krawetz
Hacker Factor
30-Oct-2014
Version 1.2

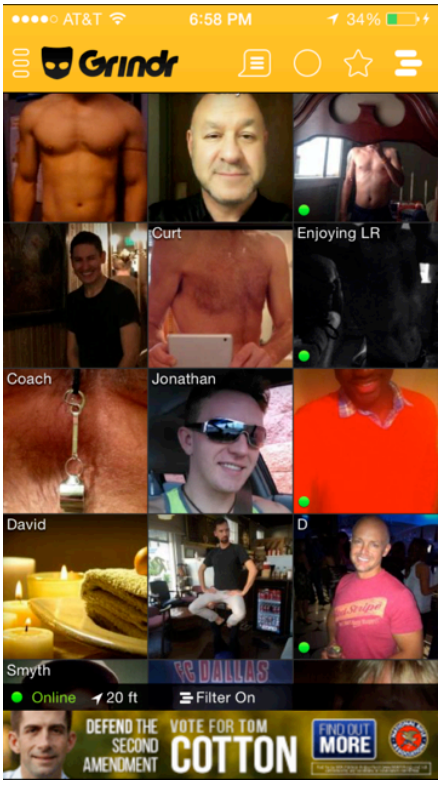
Summary

On 29-Oct-2014, Majority Strategies contacted Hacker Factor for a rapid picture evaluation. The picture is a PNG that appears to be a screenshot from an iPhone device. The suspicion raised by Majority Strategies concerns the banner ad at the bottom. Specifically, they suspect that it was digitally added. In particular, Majority Strategies identified a black bar at the top and bottom of the image that they believe is suspect.

The findings in this report conclude that the screenshot was altered and the ad was digitally inserted into the picture.

Picture Specifications

The picture provided for analysis is as follows:



File name: IMG_6385.PNG
File type: image/png
Dimensions: 359x640
Color depth: 24-bits per pixel, RGB
Aspect ratio: 16:9 – consistent with HDTV rotated.
File Size: 345,621 bytes
MD5: 33a505ca8b1d359a9387660255751981
SHA1: 88e6c367b6b0eb47978cf13e9e610a14ebba3bec

Evaluation Findings

Filename Ballistics matches the filename format to a known source. In general, users rename files less than 20% of the time; filenames typically match the source device. In this case, "IMG_6385.PNG" is a filename format used by Apple (direct from iPhone, iPad, or other mobile device) and Canon. The PNG suffix identifies that it was either captured as a PNG on an Apple mobile device or that it was a JPEG and was then converted to a PNG.

Metadata Analysis evaluates any internal metadata fields for content and consistency. In general, PNG files typically lack significant metadata fields. The only optional metadata field in this picture is a Gamma correction value of 0.454545 (also represented by its inverse: 2.2). This is a common gamma correction value. This PNG does not contain any timestamps, history, or attributions.

File Structure Ballistics evaluates the internal file format. Applications consistently generate the same internal file structures. Changes to the application's settings can alter these internal structures, but the alterations will be consistent with the application. Different applications, devices, and graphics libraries will typically generate different and well-defined structural changes. The PNG encoding settings used by this PNG are distinct. The encoding method is consistent with an Apple mobile device running iOS 5.*x* or later.

Although the file's structure can be forged, it is extremely unlikely. The file structure identifies this PNG as being encoded on an Apple mobile device running iOS 5 or later. It was not encoded by an Apple OS X, Windows, or Linux system and not encoded by any Microsoft or Adobe application.

Widget Set Identification associates the font and icons with known devices. Different mobile devices use different fonts and icons. The widget set seen at the top of the image (in the status bar) includes round dots for signal strength, service provider, WiFi icon, clock, an arrow indicating that Location Services is enabled, the batter level, and a charging symbol. This widget set is consistent with Apple iOS 7.[1] Specifically:

- iOS 7 uses circles to identify signal strength. Earlier iOS systems use bars.
- The lightning bolt symbol next to the battery, indicating charging, is specific to iOS 7.

Application Identification evaluates the content shown on the screen. This picture shows the home page of a program called "Grindr". This app is available for both iOS and Android devices. With iOS 6, the status bar above the Grindr application is the default black band. In iOS 7, the status bar is the same yellow color as the application's top bar. This screenshot is consistent with Grindr on an iOS 7 device.

---

[1] Reference: https://sites.google.com/site/appleclubfhs/support/advice-and-articles/understanding-ios-menu-symbols

Device Identification attempts to identify the device based on observed features. Different mobile devices have different screen sizes. iPhone 5, 5s, 6, and 6+ devices have a visible aspect ratio that almost exactly 16:9.[2]

A search at Google Images for "screenshot" pictures that are exactly 359x640 turned up fewer than a dozen actual iOS device screenshots; most were from Android devices. In contrast, performing the same Google search for 359x638 returned a significant number of iOS and Android screenshots. Searches for 360x640 returned some screenshots from iOS devices and many Android devices.

The device identification, application identification, file structure analysis and widget set identification strongly identify this as a screenshot from an iPhone 5, 5c, 5s, 6, or 6+ running iOS 7. The picture was captured on an iOS device and then modified on an iOS device: the picture's dimensions were increased from 359x638 to 359x640 and centered – leaving two 1-pixel thick lines along the top and bottom.

Image Analysis

PNG files are a lossless file format. Edits and modifications are not degraded during a resave. In contrast, JPEG files degrade in quality with each resave. A JPEG that is converted to a PNG will retain the JPEG compression artifacts. The IMG_6385.PNG file shows no indications of having undergone a JPEG compression.

The bottom of IMG_6385.PNG shows three regions:

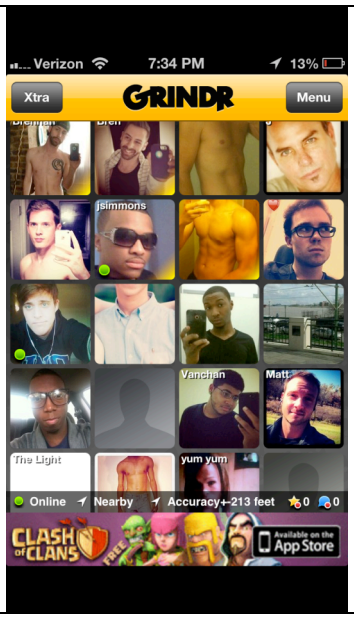
1. Images from Grindr.

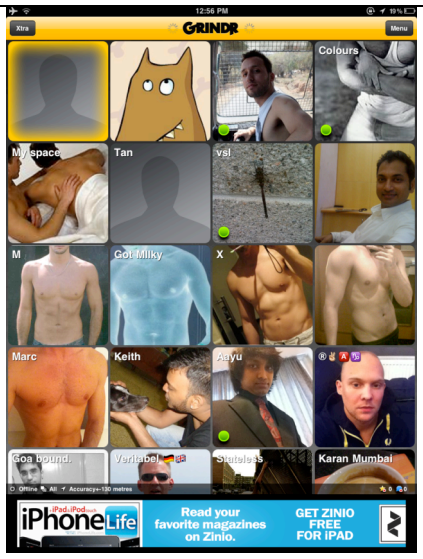
2. A black "online" status bar that is semi-transparent.

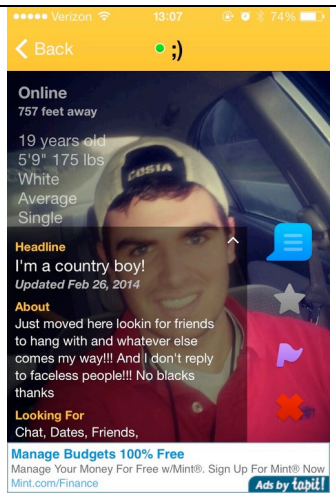
3. A banner ad. Screenshots from Grindr show that the banner ad is completely opaque and not semi-transparent.[3] In each of these examples, there is no space between the online status bar and the banner ad.

[2] Reference: http://en.wikipedia.org/wiki/List_of_iOS_devices

[3] Samples: <http://www.macpeer.com/wp-content/uploads/2011/04/IMG_0064.png>, <http://24.media.tumblr.com/8296d9037766d927ff88f00b82e62569/tumblr_n1px0tZUNP1qcttsko1_500.jpg>, <http://freethoughtblogs.com/zinniajones/files/2013/02/grindr-moore-pic-1.png>



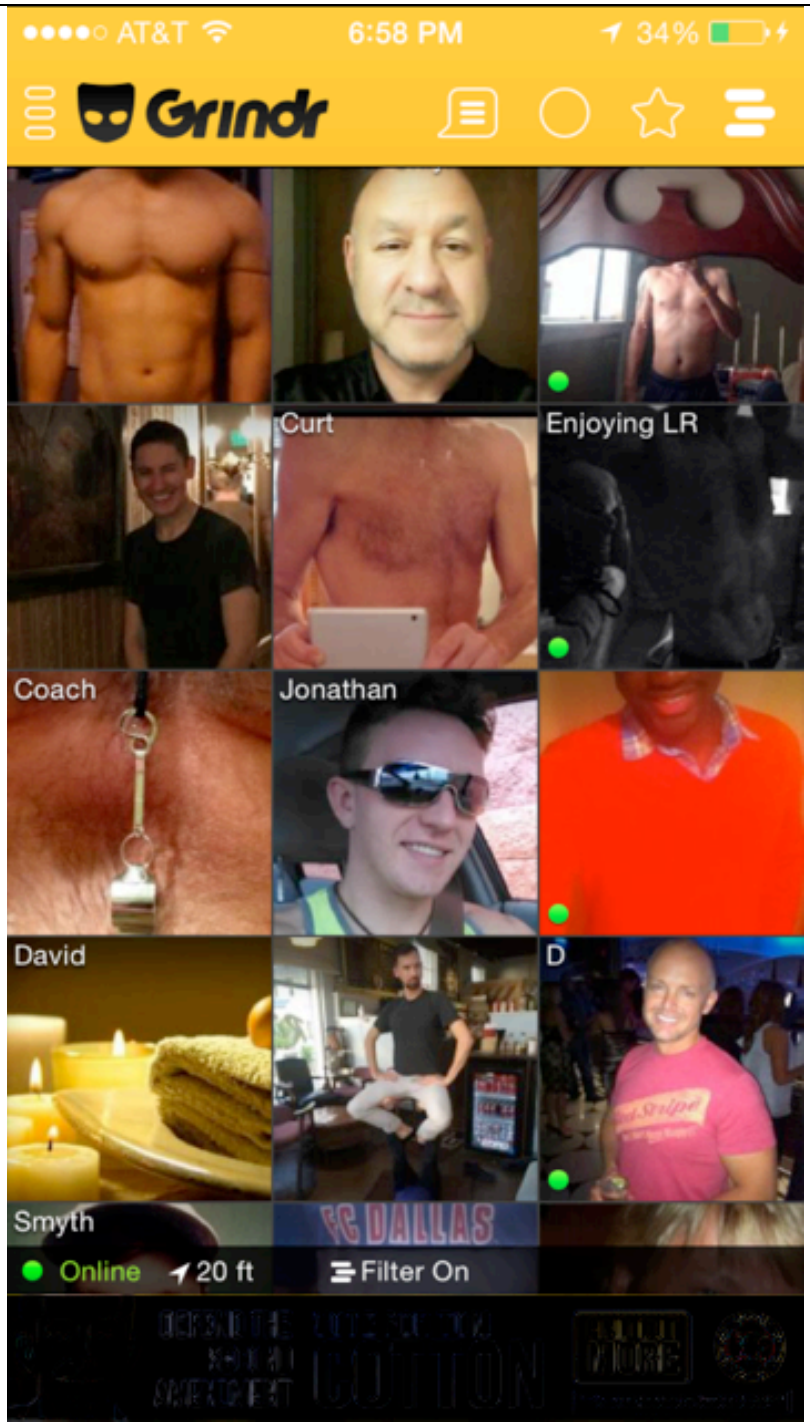




By request, Majority Strategies provided the original banner ad for comparison. The following comparison shows the original banner ad and the difference between the original ad and the ad found in IMG_6385.PNG.

The original ad was 320x50. Because IMG_6385.PNG is 359 pixels wide, the ad was scaled to match the imge. Then the difference between the scaled original and the ad in the screenshot was computed. Black indicates a perfect match in color and content, dark colors indicate a similarity, and bright colors indicate extreme difference.

This ad has been scaled from the original 320x50 to 359x56 using a bilinear scaling algorithm.



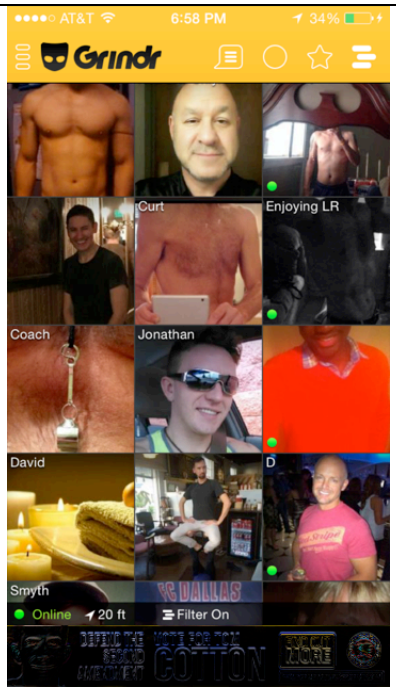
Difference between the original ad and the bilinearly scaled original ad.

The scaled original ad and the ad seen in IMG_6385.PNG shows an extremely close alignment. However, it is not a perfect alignment. The difference between the letters could be due to a variation in scaling algorithms. Bilinear and bicubic provide extremely similar results. Nearest neighbor renders a noticeably poorer match. The image was likely scaled with a variation of bilinear or bicubic scaling.

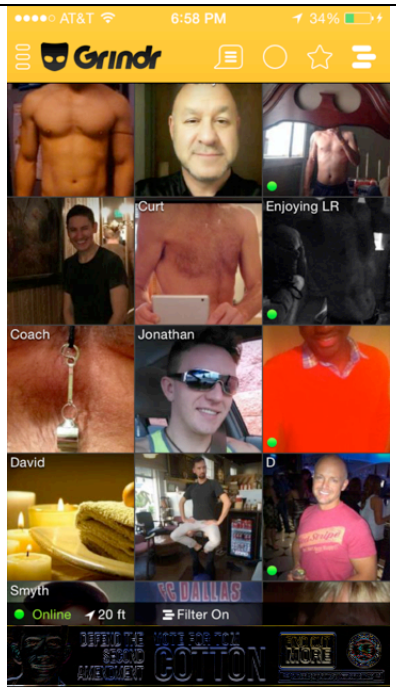
Shifting the scaled image vertically or horizontally by even one pixel results in a significantly poorer alignment on the letters, face, and other ad elements.

Aligning the bilinear-scaled image one pixel from the bottom yields a nearly perfect match to the observed greenish background, face, and most of the text. However, it is clearly one pixel short vertically. There is a single pixel line between the online status and the banner ad that does not coincide with the banner ad.

Stretching the scaled ad one pixel taller will fail to align with the text. Positioning it one pixel up will also fail to align the text.



The overlay-difference ad has been stretched vertically one pixel. The text fails to align and appears bright in the difference map.



The overlay-difference ad has been moved one pixel up. The text fails to align and appears bright in the difference map.

Regardless of the scaling, the black online status bar appears to be stretched in a way that is inconsistent with the IMG_6385.PNG ad. The misaligned row between the online status bar and the ad is not due to scaling, cropping, or alignment.

Although the misaligned row appears to be part of the banner image, it is not part of the banner image. It appears to be an extra row above the banner image. The scaled banner image ends below the misaligned row, and stretching or moving the scaled banner image to cover the row (1) fails to match the row, and (2) fails to align with the ad's contents.

The only conclusion is that the banner ad was digitally added to the screenshot. It appears as though some user pasted the banner image twice. Once with a partial blend that overlapped with

the online status bar by one pixel, and a second time with a completely opaque version that is one pixel lower.

Conclusion of Findings

Based on the analysis results, it strongly appears that the ad was digitally added to the screenshot. The events appear to be:

1. A user took a screenshot of Grindr on an iPhone 5, 5c, or 5s running iOS 7. This screenshot was saved as a PNG. The screenshot was likely 359x638.

2. An unidentified graphics program edited the picture.

3. The picture was resized to 359x640 and was vertically centered. The two black bars at the top and bottom were added to the picture.

4. A copy of the ad, likely from another screenshot, was pasted into the image. This act caused an additional line to be added between the online status bar and the ad.

5. The final version of the modified picture was saved on an Apple mobile device, running iOS 5 or later.

6. The modified picture was released to the public.

There is some ambiguity regarding the order of these events. For example, the pasting of the ad may have happened before or after the black bars were added. And different devices could have performed each step.

We can only speculate as to the motivation behind this modification. Since we are close to the 2014 elections, this could be politically motivated. For example, a rival political party may try to make an opponent look bad right before the elections, or an unrelated entity may be attacking a politician. Then again, this could be an isolated individual doing this for fun.

Additional Information

After conducting most of this analysis, the client provided added information. They stated:

- They actively block their ads from the Grindr app. So this ad should never have appeared on Grindr.

- This is an old ad that had not been used for weeks. So this ad should never have appeared anywhere recently.

- Their network logs report that this ad has not been served for this app and not served to any apps recently.

The analysis of this image supports these network results. This picture was altered and does not represent an original screenshot.