Who Decides Your Browsing Privacy?

Julian Smith, Director of Education
ANRC LLC

Professional Techniques – T31

WHAT WE ARE *NOT* GOING TO TALK ABOUT

- Which is the best browser for privacy?
- What add-ons are the most secure?
- Can I trust Google Play and the iOS app store?
- What's the risk anyway?

  (Surely my information isn't that valuable…)

WHAT WE *ARE* GOING TO TALK ABOUT

- Why track?
- HTTP User Agents
- HTTP Referrers (or is that 'Referers'*)
- Cookies
- Some tools that we can use to reveal/control browser behavior

* Infamous typo in RFC 1945 (May 1996)

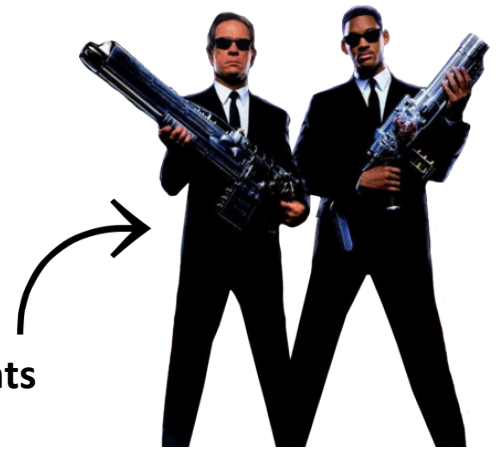
WHAT'S THE MOTIVATION?

- Advertising $$$
- Funding all of those 'free' web services
- In 2014, Google made an estimated $59bn from advertising[1]
  - Approximately 90% of their total income

[1] Source: Statista.com

USER AGENTS

- String that identifies:
  - Browser/compatibility
  - OS Platform
  - Might also include
    - Hardware
    - Plugins
- Used to provide tailored content



Not user agents

A USER AGENT STRING IN TRAFFIC

```
GET /chart/bottom HTTP/1.1
Host: www.imdb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0)Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.bing.com/search?q=worst+movies+of+all+time&qs=n&
          form=QBLH&pq=worst+movies+of+all+time&sc=8-24&sp=-1&sk=
Cookie: uu=BCYsgfw8aPz87X98E86qEVPgKI-
          f64_DpuIOrpBbN_1EZuNVwks6zStWqfeRbvWuTcW9cm5NKcH6CN899ZglJwsCrm-
          SzUdaf7I1s3Du01PZgItroId2R_8E9qVF0RmlufyNw8HQhFkaDZqV4-
          shKngE2xq6paLMzkXNwuI_0dnntj62nb7UjyMDpukWvw-
          niXcOL4C6i3v-jrFS4W66ZrFmEggixD0toGMtVltxVa5FzRDC-
          82MzLAYX7KxgftCn8oe3BsJfoliDNw_Clc06cSTVA;
          session-id=328-9994670-5212602; session-id-time=1507674670;
          __utma=68898382.662959808.1349994673.1349994673.1349994673.1;
          __utmz=68898382.1349994673.1.1.utmcsr=google|utmccn=(organic)|
          utmcmd=organic|utmctr=(not%20provided)
Connection: keep-alive
```

OTHER EXAMPLES

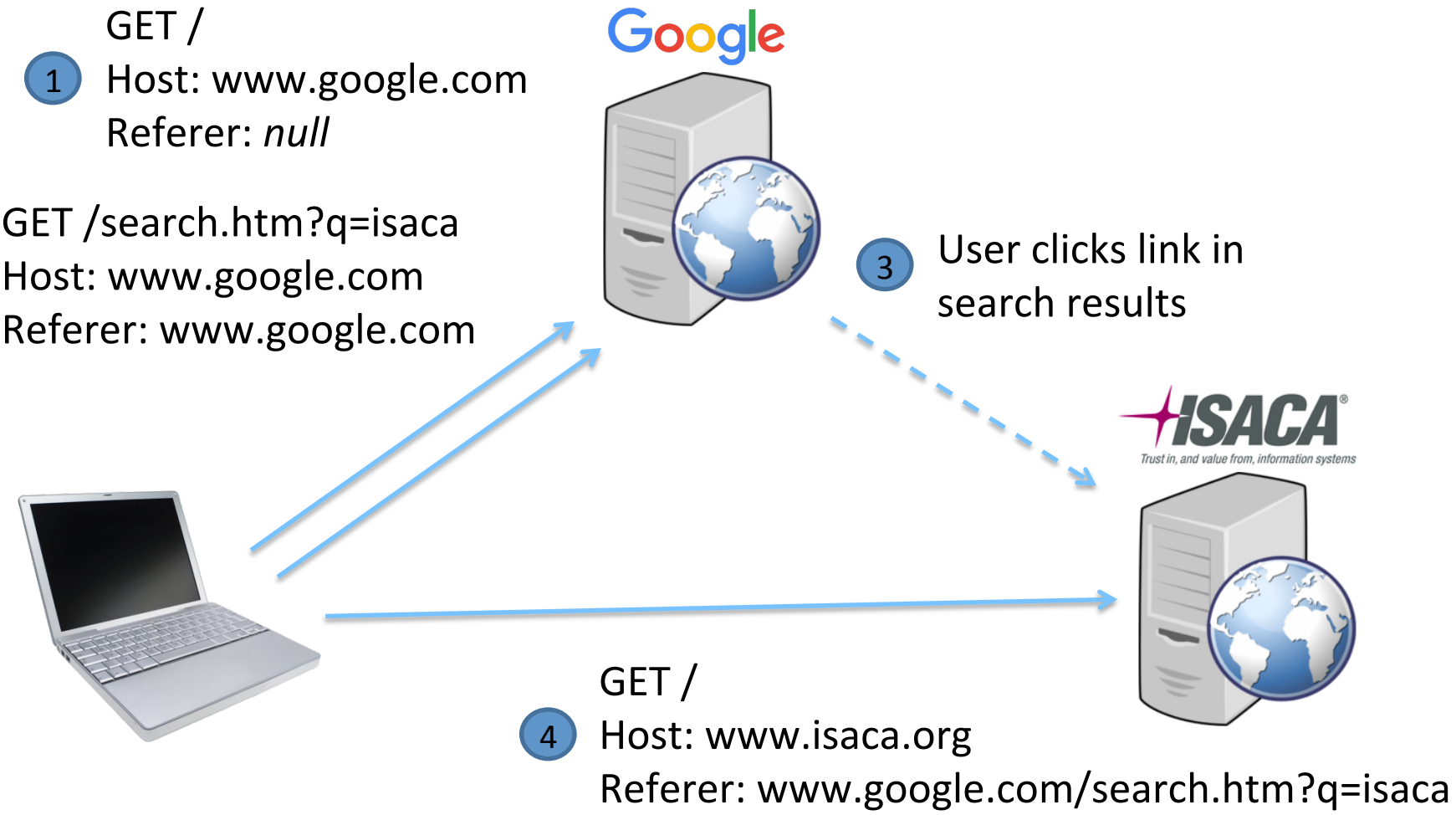
```
Mozilla/5.0 (compatible, MSIE 10.0; Windows NT 6.2;
Win64; IA64; Trident/6.0)

Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0
Mobile/10A5376e Safari/8536.25

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22
(KHTML, like Gecko) Chrome/25.0.1364.97 Safari/537.22

Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:16.0) Gecko/
20100101 Firefox/16.0
```

WHAT IS A REFERRER?

A REFERRER STRING IN TRAFFIC

```
GET /chart/bottom HTTP/1.1
Host: www.imdb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.bing.com/search?q=worst+movies+of+all+time&qs=n&
    form=QBLH&pq=worst+movies+of+all+time&sc=8-24&sp=-1&sk=
Cookie: uu=BCYsgfw8aPz87X98E86qEVPgKI-
         f64_DpuIOrpBbN_1EZuNVwks6zStWqfeRbvWuTcW9cm5NKcH6CN899ZglJwsCrm-
         SzUdaf7I1s3Du01PZgItroId2R_8E9qVF0RmlufyNw8HQhFkaDZqV4-
         shKngE2xq6paLMzkXNwuI_0dnntj62nb7UjyMDpukWvw-
         niXcOL4C6i3v-jrFS4W66ZrFmEggixD0toGMtVltxVa5FzRDC-
         82MzLAYX7KxgftCn8oe3BsJfoliDNw_Clc06cSTVA;
         session-id=328-9994670-5212602; session-id-time=1507674670;
         __utma=68898382.662959808.1349994673.1349994673.1349994673.1;
         __utmz=68898382.1349994673.1.1.utmcsr=google|utmccn=(organic)|
         utmcmd=organic|utmctr=(not%20provided)
        Connection: keep-alive
```

A WORKED EXAMPLE



HOW MUCH DOES THIS HAPPEN?

- A lot!
- Referrer-based tracking underpins pay-per-click (PPC) advertising
- Also used heavily for profiling by social media
- Let's take a look…

COOKIES

- What is a cookie?
- What types are there?
- What do/can they do?
- Who uses cookies?

WHAT IS A COOKIE?

- Originally specified in RFC 2109 (Feb 1997)
- Small amount of text (<4KB)
  - Set/updated by a server
  - Stored by your browser
  - Sent with every request to server
- Attached to a domain, e.g. google.com
- Must have a name
  - Multiple cookies are allowed per domain
  - Usually limited to 20 (browser specific)

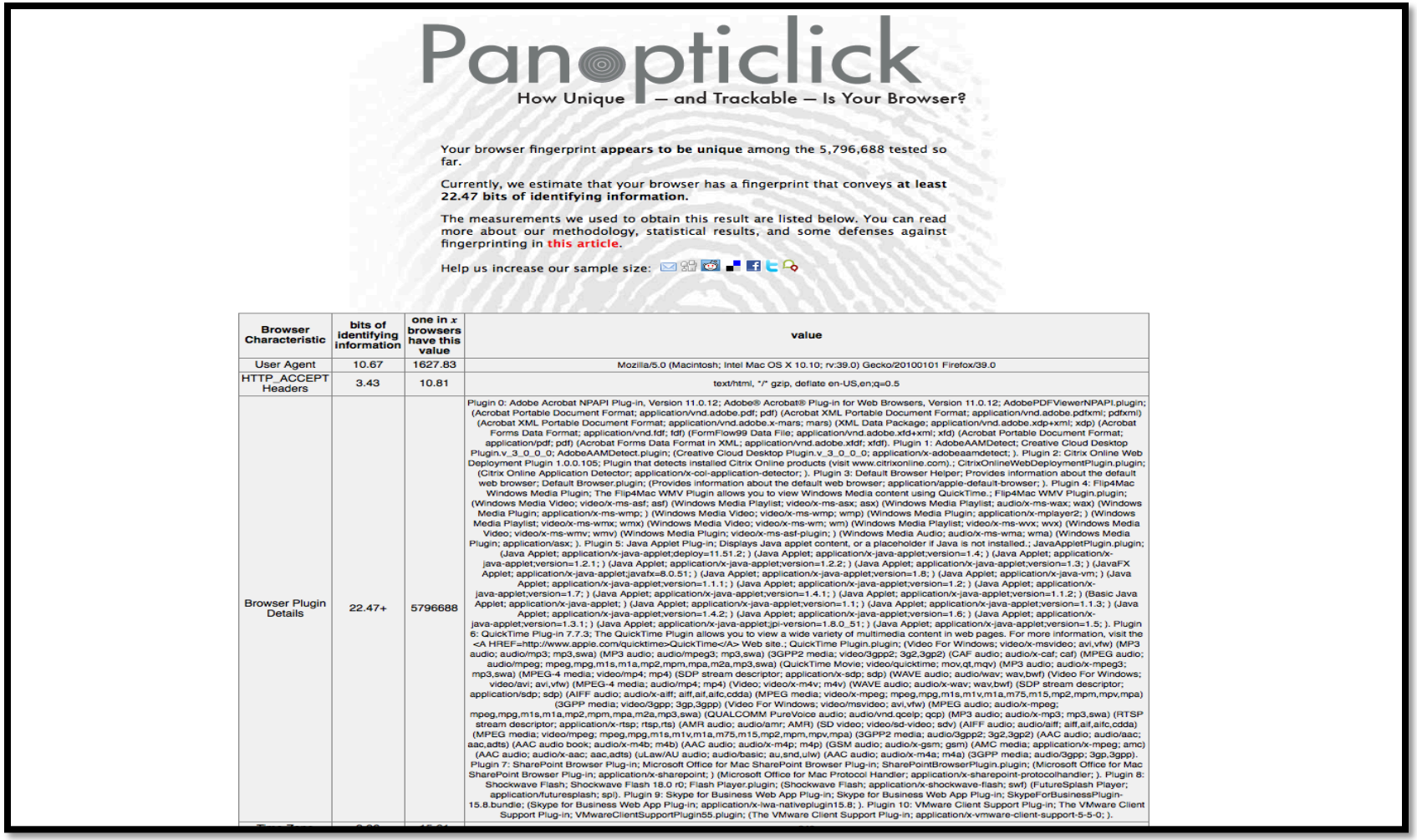
WHAT TYPES OF COOKIES ARE THERE?

- Session
- Persistent
- 'Secure' - only sent over HTTPS connection
- 3rd party
- HTTP only
  - No client-side access via (e.g.) JavaScript
- Supercookies
  - Use other technologies, e.g. Flash, to store data in the browser

COOKIES IN TRAFFIC

```
GET /chart/bottom HTTP/1.1
Host: www.imdb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/
    34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.bing.com/search?q=worst+movies+of+all+time&qs=n&
    form=QBLH&pq=worst+movies+of+all+time&sc=8-24&sp=-1&sk=
Cookie: uu=BCYsgfw8aPz87X98E86qEVPgKI-
        f64_DpuIOrpBbN_1EZuNVwks6zStWqfeRbvWuTcW9cm5NKcH6CN899ZglJwsCrm-
        SzUdaf7I1s3Du01PZgItroId2R_8E9qVF0RmlufyNw8HQhFkaDZqV4-
        shKngE2xq6paLMzkXNwuI_0dnntj62nb7UjyMDpukWvw-
        niXcOL4C6i3v-jrFS4W66ZrFmEggixD0toGMtVltxVa5FzRDC-
        82MzLAYX7KxgftCn8oe3BsJfoliDNw_Clc06cSTVA;
        session-id=328-9994670-5212602; session-id-time=1507674670;
        __utma=68898382.662959808.1349994673.1349994673.1349994673.1;
        __utmz=68898382.1349994673.1.1.utmcsr=google|utmccn=(organic)|
        utmcmd=organic|utmctr=(not%20provided)
Connection: keep-alive
```

NONE OF THE ABOVE (BROWSER FINGERPRINTING)



Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 5,796,688 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.47 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.67	1627.83	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:39.0) Gecko/20100101 Firefox/39.0
HTTP_ACCEPT Headers	3.43	10.81	text/html, */* gzip, deflate en-US,en;q=0.5
Browser Plugin Details	22.47+	5796688	Plugin 0: Adobe Acrobat NPAPI Plug-in, Version 11.0.12; Adobe® Acrobat® Plug-in for Web Browsers, Version 11.0.12; AdobePDFViewerNPAPI.plugin; (Acrobat Portable Document Format; application/vnd.adobe.pdf; pdf) (Acrobat XML Portable Document Format; application/vnd.adobe.pdfxml; pdfxml) (Acrobat XML Portable Document Format; application/vnd.adobe.x-mars; mars) (XML Data Package; application/vnd.adobe.xdp+xml; xdp) (Acrobat Forms Data Format; application/vnd.fdf; fdf) (FormFlow99 Data File; application/vnd.adobe.xfd+xml; xfd) (Acrobat Portable Document Format; application/pdf; pdf) (Acrobat Forms Data Format in XML; application/vnd.adobe.xfdf; xfdf). Plugin 1: AdobeAAMDetect; Creative Cloud Desktop Plugin.v_3_0_0_0; AdobeAAMDetect.plugin; (Creative Cloud Desktop Plugin.v_3_0_0_0; application/x-adobeaamdetect;). Plugin 2: Citrix Online Web Deployment Plugin 1.0.0.105; Plugin that detects installed Citrix Online products (visit www.citrixonline.com).; CitrixOnlineWebDeploymentPlugin.plugin; (Citrix Online Application Detector; application/x-col-application-detector;). Plugin 3: Default Browser Helper; Provides information about the default web browser; Default Browser.plugin; (Provides information about the default web browser; application/apple-default-browser;). Plugin 4: Flip4Mac Windows Media Plugin; The Flip4Mac WMV Plugin allows you to view Windows Media content using QuickTime.; Flip4Mac WMV Plugin.plugin; (Windows Media Video; video/x-ms-asf; asf) (Windows Media Playlist; video/x-ms-asx; asx) (Windows Media Playlist; audio/x-ms-wax; wax) (Windows Media Plugin; application/x-ms-wmp;) (Windows Media Video; video/x-ms-wmp; wmp) (Windows Media Plugin; application/x-mplayer2;) (Windows Media Playlist; video/x-ms-wmx; wmx) (Windows Media Video; video/x-ms-wm; wm) (Windows Media Playlist; video/x-ms-wvx; wvx) (Windows Media Video; video/x-ms-wmv; wmv) (Windows Media Plugin; video/x-ms-asf-plugin;) (Windows Media Audio; audio/x-ms-wma; wma) (Windows Media Plugin; application/asx;). Plugin 5: Java Applet Plug-in; Displays Java applet content, or a placeholder if Java is not installed.; JavaAppletPlugin.plugin; (Java Applet; application/x-java-applet;deploy=11.51.2;) (Java Applet; application/x-java-applet;version=1.4;) (Java Applet; application/x-java-applet;version=1.2.1;) (Java Applet; application/x-java-applet;version=1.2.2;) (Java Applet; application/x-java-applet;version=1.3;) (JavaFX Applet; application/x-java-applet;javafx=8.0.51;) (Java Applet; application/x-java-applet;version=1.8;) (Java Applet; application/x-java-vm;) (Java Applet; application/x-java-applet;version=1.1.1;) (Java Applet; application/x-java-applet;version=1.2;) (Java Applet; application/x-java-applet;version=1.7;) (Java Applet; application/x-java-applet;version=1.4.1;) (Java Applet; application/x-java-applet;version=1.1.2;) (Basic Java Applet; application/x-java-applet;) (Java Applet; application/x-java-applet;version=1.1;) (Java Applet; application/x-java-applet;version=1.1.3;) (Java Applet; application/x-java-applet;version=1.4.2;) (Java Applet; application/x-java-applet;version=1.6;) (Java Applet; application/x-java-applet;version=1.3.1;) (Java Applet; application/x-java-applet;jpi-version=1.8.0_51;) (Java Applet; application/x-java-applet;version=1.5;). Plugin 6: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime>QuickTime</A> Web site.; QuickTime Plugin.plugin; (Video For Windows; video/x-msvideo; avi,vfw) (MP3 audio; audio/mp3; mp3,swa) (MP3 audio; audio/mpeg3; mp3,swa) (3GPP2 media; video/3gpp2; 3g2,3gp2) (CAF audio; audio/x-caf; caf) (MPEG audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Movie; video/quicktime; mov,qt,mqv) (MP3 audio; audio/x-mpeg3; mp3,swa) (MPEG-4 media; video/mp4; mp4) (SDP stream descriptor; application/x-sdp; sdp) (WAVE audio; audio/wav; wav,bwf) (Video For Windows; video/avi; avi,vfw) (MPEG-4 media; audio/mp4; mp4) (Video; video/x-m4v; m4v) (WAVE audio; audio/x-wav; wav,bwf) (SDP stream descriptor; application/sdp; sdp) (AIFF audio; audio/x-aiff; aiff,aif,aifc,cdda) (MPEG media; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP media; video/3gpp; 3gp,3gpp) (Video For Windows; video/msvideo; avi,vfw) (MPEG audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice audio; audio/vnd.qcelp; qcp) (MP3 audio; audio/x-mp3; mp3,swa) (RTSP stream descriptor; application/x-rtsp; rtsp,rts) (AMR audio; audio/amr; AMR) (SD video; video/sd-video; sdv) (AIFF audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG media; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2 media; audio/3gpp2; 3g2,3gp2) (AAC audio; audio/aac; aac,adts) (AAC audio book; audio/x-m4b; m4b) (AAC audio; audio/x-m4p; m4p) (GSM audio; audio/x-gsm; gsm) (AMC media; application/x-mpeg; amc) (AAC audio; audio/x-aac; aac,adts) (uLaw/AU audio; audio/basic; au,snd,ulw) (AAC audio; audio/x-m4a; m4a) (3GPP media; audio/3gpp; 3gp,3gpp). Plugin 7: SharePoint Browser Plug-in; Microsoft Office for Mac SharePoint Browser Plug-in; SharePointBrowserPlugin.plugin; (Microsoft Office for Mac SharePoint Browser Plug-in; application/x-sharepoint;) (Microsoft Office for Mac Protocol Handler; application/x-sharepoint-protocolhandler;). Plugin 8: Shockwave Flash; Shockwave Flash 18.0 r0; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 9: Skype for Business Web App Plug-in; Skype for Business Web App Plug-in; SkypeForBusinessPlugin-15.8.bundle; (Skype for Business Web App Plug-in; application/x-lwa-nativeplugin15.8;). Plugin 10: VMware Client Support Plug-in; The VMware Client Support Plug-in; VMwareClientSupportPlugin55.plugin; (The VMware Client Support Plug-in; application/x-vmware-client-support-5-5-0;).

HANDS-ON TIME!

- Please open your laptops
- Are you ready to try your hand as a network forensics analyst?