**使用 Wireshark 和 Debookee 进行 Android 网络数据包监控和分析**

Mi-Hwa Song

Division of Information and communication technology, Semyung University, Jechon, Korea e-mail: mhsong@semyung.ac.kr

**摘要**

近年，由于智能手机和智能平板电脑等智能设备的部署，移动流量大幅增加。Android 是全球智能手机中功能最强大的移动平台。Android 操作系统提供对许多应用程序和 Internet 的无缝访问。它将涉及通过网络通信的网络数据包共享。网络数据包包含许多有关网络活动的有用信息，可用作一般网络行为的描述。为了研究网络数据包的行为，网络管理员使用网络数据包分析软件等有效的工具来捕获和分析网络信息。在这项研究中，更多地了解从 Android 智能手机捕获的实时网络数据包中的网络信息是目标，并确定最佳的网络分析仪软件。

**关键词**：网络包监控、安卓网络监控、网络包分析软件、安卓平台。

1. **简介**

智能手机正在稳步普及，随着它们在计算能力、传感器和通信方面的能力增加，创造了新的应用领域。智能手机流量在互联网流量中所占份额显着增加。预计蜂窝流量的增长速度将比固定互联网流量快 10 倍，其中大部分流量由智能手机产生。Android 是针对智能手机的较新操作系统之一，但已导致蜂窝网络流量的爆炸性增长。由于 Facebook、Skype、网上银行、电子邮件客户端等应用程序的普及，移动设备通常用于浏览互联网的各种应用程序，这些应用程序不断与相应的服务器交换数据。在蜂窝网络中，移动设备通过网络进行通信以共享资源和数据。网络数据包是在这些网络中传输的数据单元，它们将所有重要信息从源头传送到最终目的地。当我们使用网络浏览器（如 Google 或 Naver 搜索门户）使用 Android 设备浏览 Internet 时，我们只需单击链接，网站将在一秒钟内出现。

我们不知道有数据包和协议发生了交换，并且在这之后发生了什么过程。我们如何使用这些数据包来了解网络中发生了什么？

要研究网络实时数据包背后发生的所有过程，我们需要一个特定的软件来捕获和分析网络数据包。有许多网络数据包分析工具可用，但我们还不知道哪些软件可以在网络数据包捕获和分析中提供最佳性能。我们也不知道可以从Android设备上的实时网络中的网络数据包捕获和分析中检索到哪些信息。

基于上述问题，本研究的目标是:

1) 研究从网络分析仪中检索到的实时网络数据包信息

2) 确定什么是最好的网络数据包分析工具

3) 对至少两种不同的网络数据包分析工具进行比较

为了探索和了解网络分析软件捕获的网络数据包分析信息。本研究将侧重于:

* Android网络数据包分析
* Debokee and Wireshark (网络数据包分析软件)
* 分析捕获的网络数据包

1. **背景**

本主题是对过去和进展研究的回顾。它包括对数据包分析、数据包分析工具软件、Android 网络数据包分析工具、基于 Android 的智能手机的评论以及与研究相关的所有评论。

2.1 数据包分析

数据包分析，也称为协议分析、网络分析、流量分析、数据包嗅探、窃听等，是捕获网络数据包并从网络信息中学习以确定网络上发生了什么的过程。它还涉及通过在数据网络上两个实体之间交换协议数据单元，对使用预定协议进行的选定通信进行监视过程。根据 Spangler 和 Ryan 的说法，数据包嗅探是一种监控通过网络的每个数据包的技术[1]。

2.2 数据包分析工具

数据包分析工具或也可以识别为协议分析工具或数据包嗅探器或数据包分析工具是监视通过网络传输的数据包的程序/软件。该软件将网络流量中常见协议的数据包解码为可读格式的网络信息。本发明的协议分析工具能够显示站级统计、网络统计、实时事件信息和协议分布。它还用于实时计算和显示与数字传输网络上承载的数据帧相关的协议分布[2]。数据包嗅探器是监控所有网络流量的硬件或软件，可以在交换和非交换环境中运行 [3]。

有许多数据包分析工具可帮助管理员的工作变得更加轻松。在 Internet 上进行简单搜索即可显示适用于 Windows OS 或 Mac OS 的分析仪数量。数据包分析工具也可以直接在某些智能手机本身上安装和访问。一些最突出的是：

* Wireshark

Wireshark 是可用的最好的嗅探器之一，并且正在作为免费的、商业质量的嗅探器开发。它具有众多功能、漂亮的图形用户界面 (GUI)、解码 400 多种协议，并且正在积极地开发和维护。它运行在基于 UNIX 的系统、Mac OS X 和 Windows 上。这是在生产环境中使用的一个很好的嗅探器。

* Debookee

Debookee 是 OS X 的数据包分析工具，能够通过中间人攻击拦截网络流量。Debookee 将拦截来自网络上任何设备的流量，包括 iPhone、iPad、Android、Blackberry、PC、Mac 等。这使用户能够分析不支持数据包捕获的设备的流量，例如移动设备、平板电脑等。在没有网络中断的情况下，Debookee 可以完成对您的网络的扫描并显示与发现相关的 IP 地址、MAC 地址和供应商 设备。

* PRTG Network Monitor

PRTG 网络监控器是 Paessler AG 的网络监控软件。PRTG 在 Windows 上运行，并使用 SNMP、数据包嗅探、WMI、IP SLA 和 Netflow 以及各种其他协议监控网络可用性和网络使用情况。自 PRTG 9 版本发布以来，该软件支持对 IPv6 设备的监控。提供基于 Web 的界面，以及适用于 iOS 和 Android 的专用应用程序。

* Ettercap

Ettercap 专门设计用于嗅探交换网络。它具有密码收集、操作系统指纹识别和字符注入等内置功能，可在包括 Linux、Windows 和 Solaris 在内的多个平台上运行。它由 ettercap.sourceforge.net 积极维护。

* Tcpdump

Tcpdump 是最古老和最常用的网络嗅探器，由劳伦斯伯克利国家实验室 (LBNL) 信息与计算科学部 (ICSD) 的网络研究组 (NRG) 开发。它基于命令行并在基于 UNIX 的系统（包括 Mac OS X）上运行。它由 www.tcpdump.org 积极开发和维护。

据 ibm.com 称，Wireshark 是迄今为止最好的基于 GUI 的开源数据包分析工具 [4]。该工具对于网络管理员了解所有计算机正在尝试与机器通信的详细信息非常有帮助。Wireshark 也在最佳免费网络分析工具列表中 [5]。事实上，Wireshark 通常被认为是业界事实上的标准。

Debookee 在友好的图形用户界面中提供实时数据包捕获分析。Debookee 不会用 RAW 数据包压倒用户，而是仅显示通常在数据包流中发现的最重要和最通俗的信息。因此，Debookee 支持从 HTTP、HTTPS、DNS、TCP、DHCP、SIP 和 RTP 协议中提取请求详细信息。Debookee 通过三个简单的步骤 [6] 分析任何设备的网络流量。首先，Debookee 扫描网络并识别正在使用的设备。然后用户选择他们想要分析的设备或目标。只需单击一下，Debookee 即可提供全面的报告，以便用户分析流量。

2.3 监控安卓设备的网络数据包

如今，用于移动设备的操作系统 Android 在智能手机和平板电脑领域处于领先地位。Android 是谷歌的移动设备操作系统。从这个意义上说，最常用的功能之一是能够通过互联网连接在两个设备之间传输数据。

2.3.1 Android平台模拟数据流量分析与解读 [7]

最终目标是了解 Android 如何管理发送和接收数据包。为此，在进行了所有必要的测试后，对结果进行深入分析，以凭经验得出哪种连接类型最适合传输不同流量类型，而 Wi-Fi 是传输它们的最佳选择。在不久的将来，应用程序将能够利用这些知识优化其性能。从实际测试中得到的结果，将得出关于Android如何处理数据包的发送和接收的结论。这些结论将针对每种连接类型，分别分析模拟器、Wi-Fi 和 3G。

2.3.2 监控安卓设备的网络流量 [8]

组织用于监控进入其网络的网络流量的相同原则必须应用于源自移动设备的网络流量。这意味着通常用于收集和分析网络活动的技术和工具也可用于检测与智能手机相关的异常网络流量或网络入侵。

2.3.3 使用交互式实验室的 Android 平台的 Android 恶意软件行为

随着操作系统的发展，Android 的恶意软件也急剧增加。目前，很少有策略可用于识别和检测该平台上的恶意软件。它包含网络数据包分析策略，可以帮助识别可能的攻击或恶意活动或查找不安全和臃肿的应用程序。本文详细讨论了作者为使学生熟悉Android平台和动态恶意软件分析技术而开发的四个技术。

总之，网络数据包分析方法在以前的实验中被广泛用于监控在网络上传输的数据包活动。该方法还有助于识别网络中发生的恶意软件行为或任何可能的攻击活动。有许多网络数据包分析工具可以帮助实现网络数据包分析。根据许多评论，Wireshark 是当今最好和常用的网络分析仪。

1. **研究方法论**

3.1 Android上数据包分析的分析框架

在执行数据包分析时，通常大部分分析将在捕获之后进行。有时需要执行多次捕获才能获得更好的观察结果。从第一个开始捕获网络数据包直到获得分析结果，需要做的过程很少。图1 显示了数据包分析工具的流程是如何完成的。本研究中使用了两种数据包分析工具，即 Wireshark 和 Debookee。两种网络数据包分析软件的流程如图1所示。

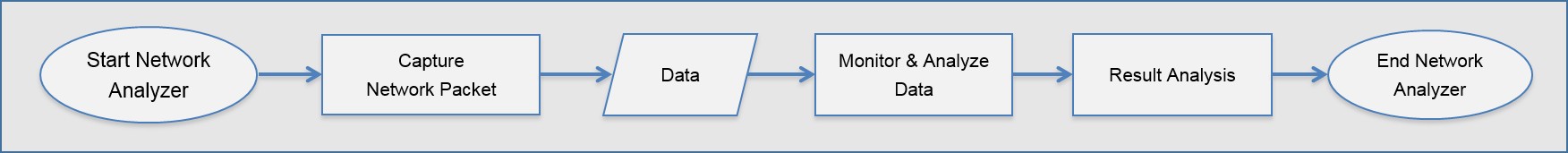


图1. 分析流程图

3.2 系统架构

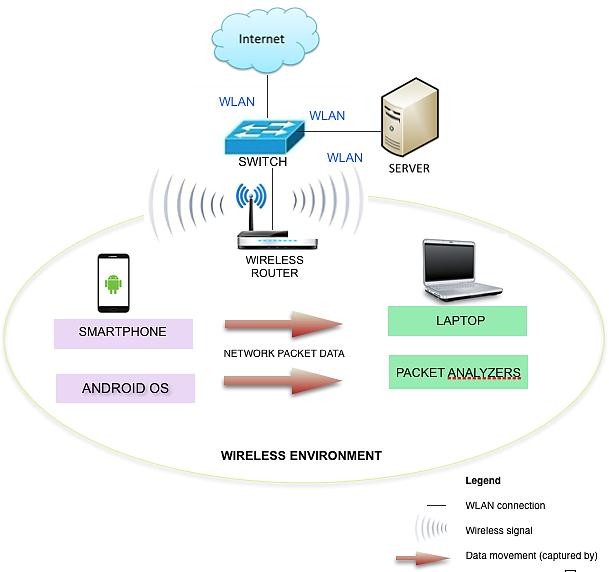


图2. Android 网络数据包分析系统架构

图2 显示了 Android 智能手机系统架构中的网络数据包分析。该图显示了分析过程中涉及的所有组件和连接。本研究使用的连接是无线连接，智能手机和笔记本电脑连接在同一无线网络中。无线连接是从连接到主要来源 Internet 的无线路由器建立的。笔记本电脑中安装了 Wireshark 和 Debokee 两个数据包分析工具，用于捕获、监控和分析来自智能手机的网络数据包。分析工具将捕获来自智能手机的网络数据包数据。

3.3 硬件和软件

这项研究需要一些软件和硬件来实现研究目标。需要的软件和硬件清单：

软件：Wireshark, Debookee, Android 操作系统

硬件：Android 手机, 笔记本电脑, 无线路由器

3.4 设置过程



图3. 设置过程

本研究中的设置过程很简单，如图3 所示。无线路由器用于向笔记本电脑和 Android 智能手机分配无线连接。无线路由器的 SSID（服务集标识符）名称是“TPLINK”。然后，笔记本电脑和 Android 智能手机从无线路由器连接到相同的无线连接。智能手机将浏览互联网活动，例如发送电子邮件、网上银行、社交网络等，而安装在笔记本电脑中的 Wireshark 和 Debookee 网络分析器将捕获和监控来自智能手机的网络数据包数据。最后，网络分析器将进行分析并从数据包数据中检索网络信息。

3.4.1 安装 Wireshark

在这项研究中，wireshark 是用于捕获和分析网络数据包数据的网络分析器之一。Wireshark 是有用的数据包工具之一。Wireshark 的一些特性：

* 它具有易读和可配置的 GUI
* 它可以从网络捕获数据或从捕获文件中读取
* 具有丰富的显示过滤功能

Wireshark 可以安装在 Windows 和 Mac 操作系统上。首先，从其官方网站（www.wireshark.org）[9] 下载 Wireshark 软件。然后，按照所有安装说明将其安装到笔记本电脑中，直到安装完成。Wireshark的几个界面如下图4。

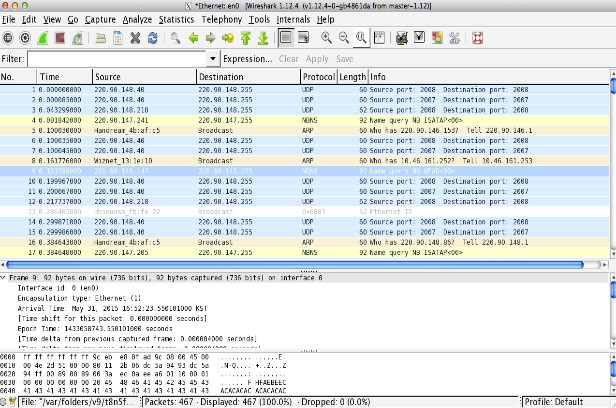
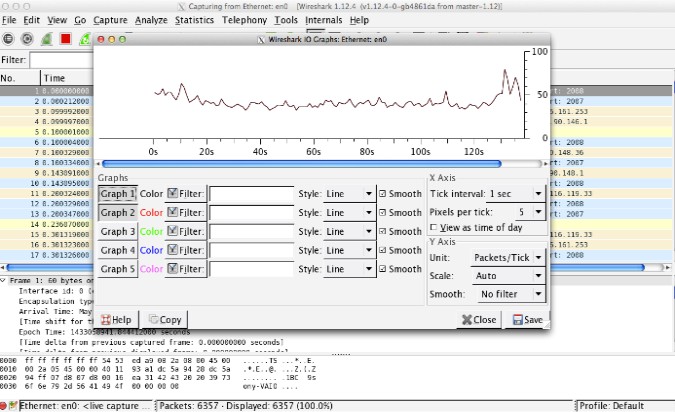


图4. Wireshark 网络抓包接口（左）、IO 图（右）

3.4.2 安装 Debookee

Debookee 是本研究中使用的另一种网络分析仪。Debookee 是专为 Mac OS X 设计的数据包分析器。它在网络分析器软件中仍然是新的。使用 Debookee 软件是因为想探索它的特性，并将其与 Wireshark 的性能进行比较。Debookee 提供的一些功能是：

* 扫描并发现网络上当前处于活动状态的所有设备
* HTTP、HTTPS、DNS、TCP、DHCP、SIP等协议的实时抓包分析

Debookee 只能安装在 Mac OS X 操作系统上。首先，从其官方网站（ww.iwaxx.com）下载 Debookee 软件[10]。然后，按照所有安装说明将其安装到笔记本电脑中，直到安装完成。下面图5和图6有几个Debookee的界面。

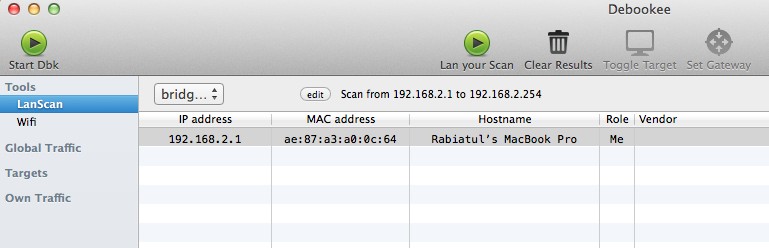


图5. Debookee的启动界面（左），Debookee的Wifi界面（右）

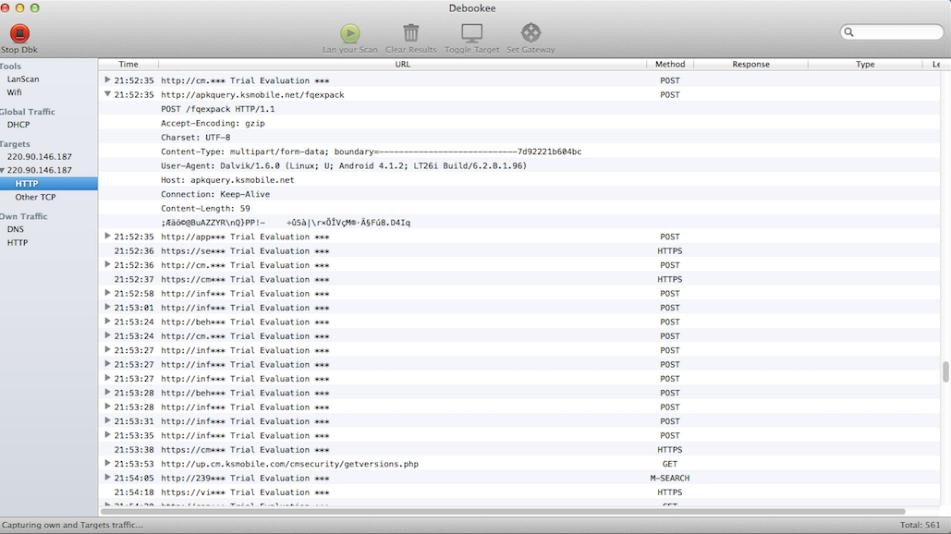


图6. Debookee的网络数据包捕获接口

1. **结果和分析**

本章讨论从网络分析仪 Wireshark 和 Debookee 捕获的网络数据包数据的结果和分析。每个检索到的网络信息都会有解释。进行分析以研究 Wireshark 和 Debookee 之间最好的网络分析仪及其比较。

4.1 Wireshark 分析

1) 浏览视频 ([www.youtube.com](http://www.youtube.com))

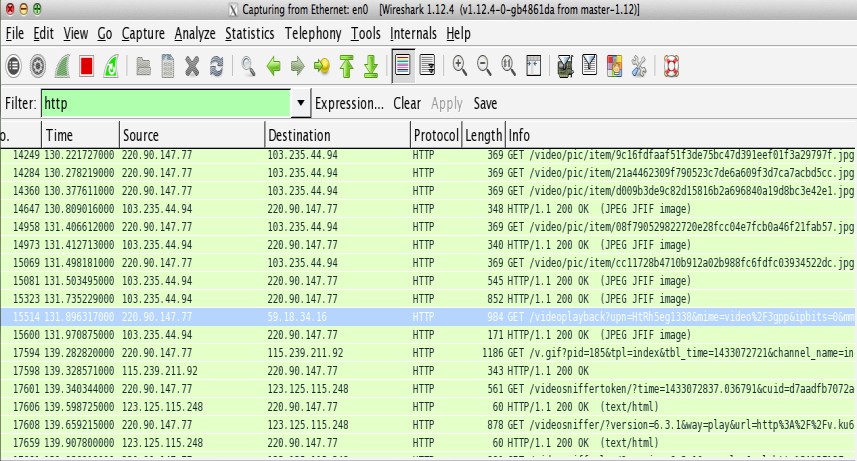


图7. 在 youtube 上观看视频 (左),Wireshark 数据包列表从 youtube 观看视频 (右)

Wireshark 开始捕获来自观看 youtube 视频的网络数据包数据。图8 可以显示包含当前捕获文件中的所有数据包、数据包编号、捕获数据包的相对时间、数据包的来源和目标以及数据包的协议的表格摘要。

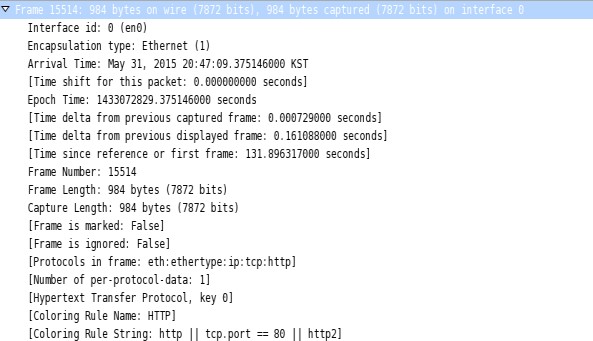


图8. 数据包详细信息（帧详细信息）

从图8 中检索到的信息摘要是：

* 包的帧号：15514
* 协议：HTTP
* 接口 id： 0
* 封装类型：以太网
* 数据包帧的到达时间：2015 年 5 月 31 日 20:47
* 数据包的时延：0.000000000秒
* 帧长 : 984 bytes

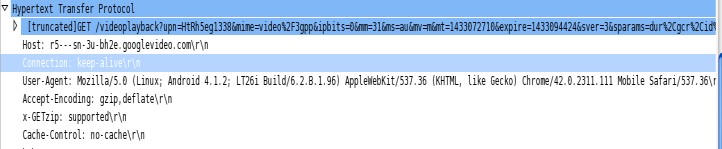
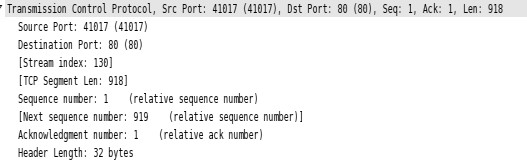


图9. 数据包详细信息（TCP 详细信息）和数据包详细信息（HTTP 详细信息）

从图9（TCP 详细信息）检索到的信息摘要是：

* 源端口号：41017
* 目的端口：80
* Ack 应答序号：1
* Seq序号：1
* 头部长度：32 bytes

从图9（HTTP 详细信息）检索到的信息摘要是：

* 方法： GET
* 连接方式： keep-alive (长连接)
* 用户标识 : Mozilla/5.0 ( Linux; Android 4.1.2)

2) 网上银行 (www.cimbclicks.com.my)

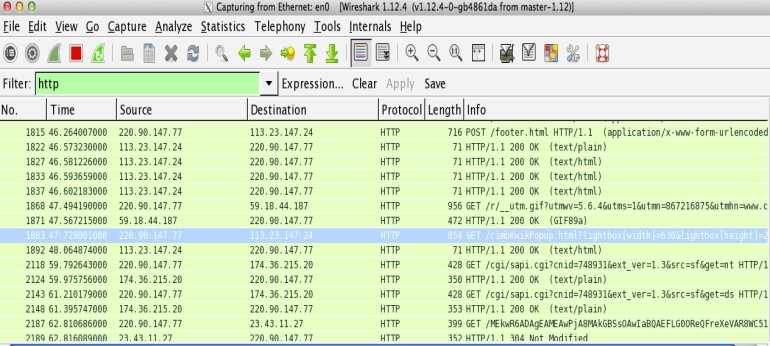


图10. CIMB网上银行服务（左），CIMB在线产生的 Wireshark 数据包(右)

Wireshark 开始捕获来自网上银行服务的网络数据包数据。

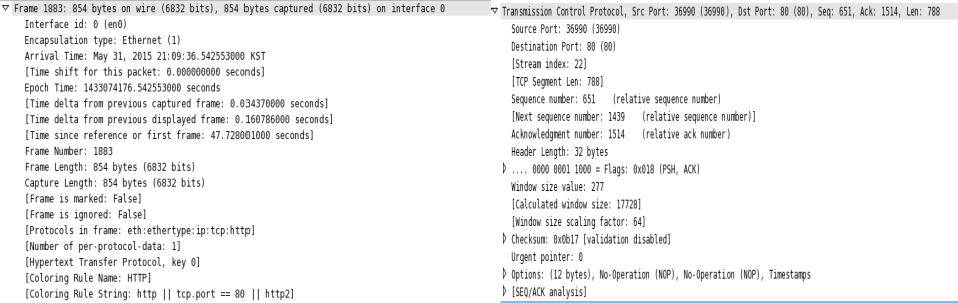


图11. 数据包详细信息（帧详细信息）和数据包详细信息（TCP 详细信息）

从图11（帧细节）检索到的信息摘要是：

* 帧号：1883
* 协议HTTP
* 接口 id：0
* 封装类型：Ethernet
* 抵达时间：2015 年 5 月 31 日 21:09
* 包时延：0.00000000 秒
* 帧长：854 bytes

从图11（TCP 详细信息）检索到的信息摘要是：

* 源端口号：36990
* 目的端口：80
* Ack确认号：1514
* Seq请求号：651
* 首部长度：32 bytes
* TCP 段长度：788

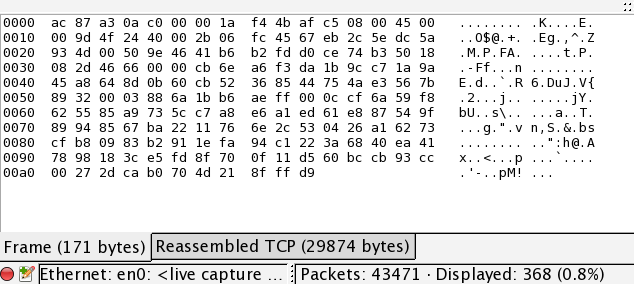
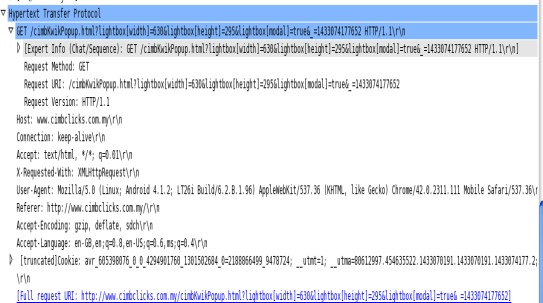


图12. 数据包详细信息（HTTP 详细信息）（左）和数据包字节数（右）

从图12（HTTP 详细信息）检索到的信息摘要是：

* 方法：GET
* 对方： [www.cimbclicks.com.my](http://www.cimbclicks.com.my)
* 连接方式：keep-alive (长连接)
* 接收：text/html
* 用户标识：Mozilla/5.0 (Linux; Android 4.1.2)

数据包字节（图12（右））以原始、未处理的形式显示数据包。图12（右）的右侧部分以 ASCII 字符显示了每个数据包的内容

4.2 Debookee’s 分析

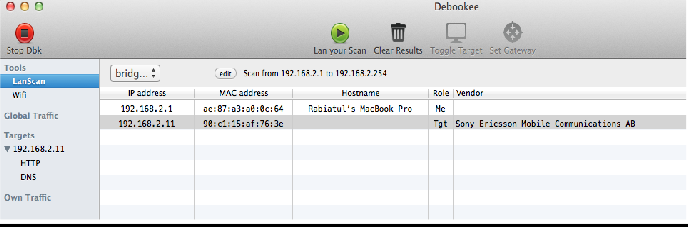


图13. Debookee 在活动网络中的设备列表

图13 显示了在同一网络中活动的设备列表。有两种设备，Android智能手机就是其中之一。界面显示设备的 IP 地址、MAC 地址、主机名和供应商。智能手机的 IP 地址为 192.168.2.11，供应商名称为 Sony Ericsson Mobile Communication AB。

1. 浏览视频 (www.youtube.com)

智能手机浏览 youtube.com 的图与上图相同。（参考图10.）

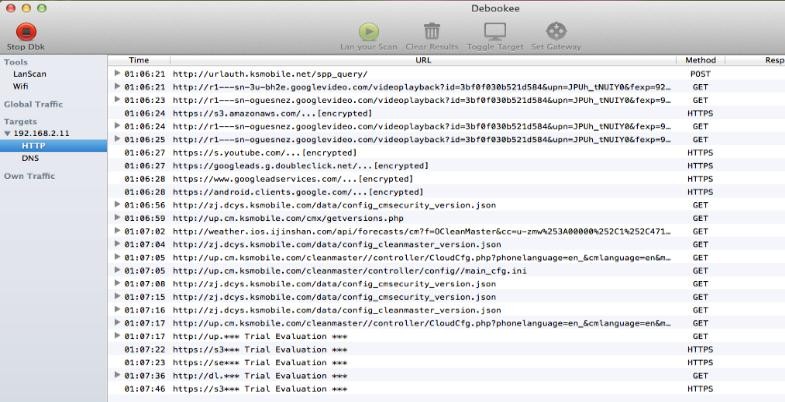


图14. Debookee 的数据包列表

图14 可以显示数据包的时间、URL、方法、响应、类型和长度的摘要。 从智能手机浏览 youtube.com 时捕获的方法很少。 方法是：

* POST 方法 (HTTP 请求方法)：请求 Web 服务器接受包含在请求消息正文中的数据以进行存储。 它通常在上传文件或提交完整的 Web 表单时使用
* GET 方法 (HTTP 请求方法)：旨在检索一些数据，并且只能向服务器发送有限数量的参数数据。
* HTTPS (安全超文本传输协议)：HTTP 的安全版本，即在您的浏览器和您连接的网站之间发送数据的协议。

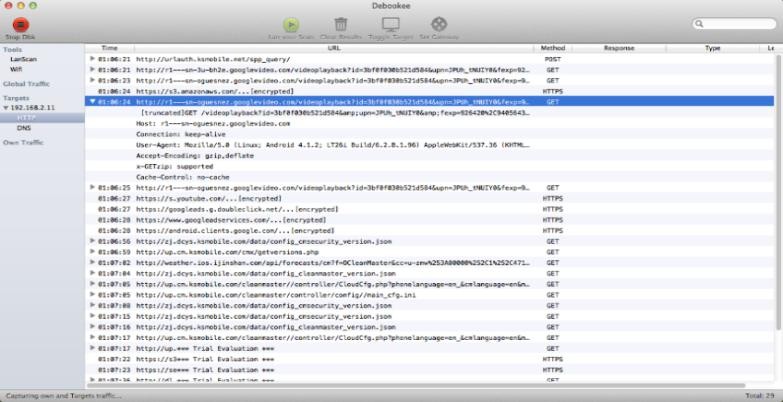


图15. youtube.com 数据包详细信息

图15 可能显示以下内容的摘要：

* 方法：GET
* 对方：googlevideo.com
* 连接方式：keep-alive
* 用户标识：Mozilla/5.0 (Linux; Android 4.1.2)
* 接收编码：gzip (文件格式和用于文件压缩和解压缩的软件应用程序)

2) 网上银行 (www.cimbclicks.com.my)

智能手机浏览 cimbclicks 的图与上图相同。（图15）

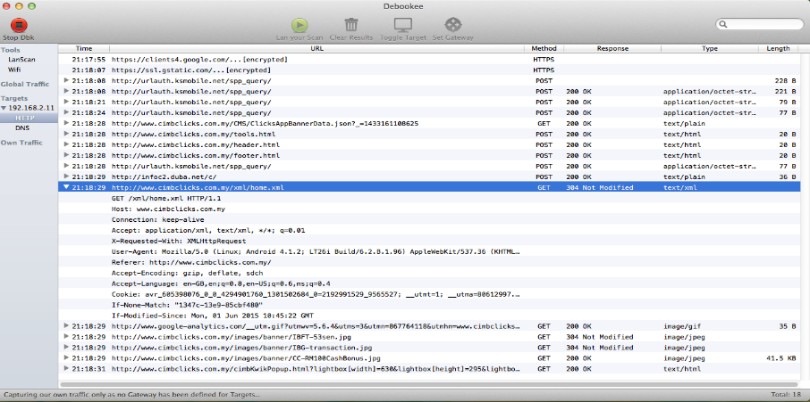


图16. cimbclicks.com.my 数据包详细信息

图16 可能显示以下内容的摘要：

* 方法：GET
* 返回：304 Not Modified (请求的 URL 的资源自上次访问或缓存后未更改).
* 对方：[www.cimbclicks.com.my](http://www.cimbclicks.com.my)
* 连接方式：keep-alive
* 接收: application/xml, text/xml
* 用户标识：Mozilla/5.0 (Linux; Android 4.1.2
* 接收编码：gzip
* 接收语言：en-GB (Great Britain English language), en (English), en-US (United States English Language)
  1. Wireshark 与 Debookee 对比

|  |  |  |
| --- | --- | --- |
|  | Wireshark | Debookee |
| 界面 | 复杂，但用户友好 | 简单 |
| 平台 | Windows, Mac X OS | Mac X OS |
| 一致性 | 应用广泛，最好的网络分析工具 | 不常用，新包分析工具 |
| 费用 | 免费(开源) | 有限功能免费，完整版 30 美元 |
| 功能性 | 功能多，网络信息详解 | 功能少，网络信息少 |

表1. Wireshark 与 Debookee 对比表

1. **总结**

网络分析仪是捕获来自同一网络中各种设备的网络数据包的最佳工具。然后，需要分析网络数据包以了解其中包含哪些信息。使用最好的网络分析仪对于获取更多网络信息的细节非常重要。

根据分析，Wireshark 和 Debookee 两种网络分析器都会生成有关捕获的网络数据包的信息。但是 Wireshark 相比 Debookee 分析了捕获网络数据包的更多细节。例如，分析非常详细的帧数据包部分，传输控制协议（TCP）部分，超文本传输协议等等可以探索。Wireshark 中提供的功能比 Debookee 中的功能更多。例如，Wireshark 还提供 IO Graph、协议过滤器、电话等。Debookee 只提供基本功能，但它仍然有用，但不像 Wireshark 那样详细。

分析显示了包数据中涉及的许多网络信息，帮助用户了解正在使用的方法、包的到达时间、包的长度、谁是用户代理，并且可以看透网络包过程中真正发生的事情。该分析有助于用户了解网络数据包流程的流程。

**引用**

[1] Spangler, R. “Packet sniffer detection with antisniff”. University of Wisconsin - Whitewater. Department of Computer and Network Administration, 2003.

[2] Anderson, C. D., Anderson, M. B., Cookmeyer, E. N., Daniels, R. A., Wheat, L. E., & Lingle, R. A.. U.S. Patent No. 5,850,388. Washington, DC: U.S. Patent and Trademark Office., 1998.

[3] Rupam, Atul Verma, Ankita Singh. “An Approach to Dectect Packets Using Packet Sniffing”, International Journal of Computer Science & Engineering Survery(IJCSES), Vol 4, No. 3., 2013.

[4] Wireshark is best GUI packet analyzer, http://ibm.com, 2012.

[5] Wireshark tool – best free network analyzer , http://techsupportalert.com, 2015.

[6] Debookee analyzer, http://prmac.com, 2014.

[7] Arias, A. C. “Analysis and interpretation of emulated data traffic in Android platform”, Vienna University of Technology, Department of Electrical Engineering, 2011.

[8] Parrizas, A. A. “Monitoring network traffic for Android device”, GIAC(GCIA) Gold Certification, SANS Institute InfoSec Reading Room., 2013.

[9] Wireshark, http://www. wireshark.org

[10] Debookee, http://www. iwaxx.com