

## Ex.8 Penetration Testing Activity 4

**Name:** Vinayak Kumar Singh

**Reg No:** 23MCA1030

**Subject:** Software Testing

1. What is the MAC address of Ann's AppleTV?

**Ans:** (00:25:00:fe:07:c4)

```
Ethernet II, Src: Apple_fe:07:c4 (00:25:00:fe:07:c4), Dst: CiscoLinksys_ad:57:7b (00:23:69:ad:57:7b)
  Destination: CiscoLinksys_ad:57:7b (00:23:69:ad:57:7b)
    Address: CiscoLinksys_ad:57:7b (00:23:69:ad:57:7b)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0 .... = IG bit: Individual address (unicast)
  Source: Apple_fe:07:c4 (00:25:00:fe:07:c4)
    Address: Apple_fe:07:c4 (00:25:00:fe:07:c4)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

2. What User-Agent string did Ann's AppleTV use in HTTP requests?

**Ans:** AppleTV/2.4

Search HTTP and Follow HTTP Stream Path

```
Wireshark · Follow HTTP Stream (tcp.stream eq 0) · evidence03.pcap

GET /WebObjects/MZStore.woa/wa/viewGrouping?id=39 HTTP/1.1
Accept: */*
Accept-Language: en
Accept-Encoding: gzip, deflate
Cookie: s_vi=[CS]v1|259C176A85010C29-6000010D80115D7F[CE]
User-Agent: AppleTV/2.4
If-Modified-Since: Fri, 25 Dec 2009 04:42:31 GMT
X-Apple-Store-Front: 143441-1,3
Connection: keep-alive
Host: ax.itunes.apple.com
```

3. What were Ann's first four search terms on the AppleTV (all incremental searches count)?

**Ans:** h, ha, hac, hack

http.request.method == "GET" && ip.dst == 66.235.132.121

Filter : http.request.uri contains

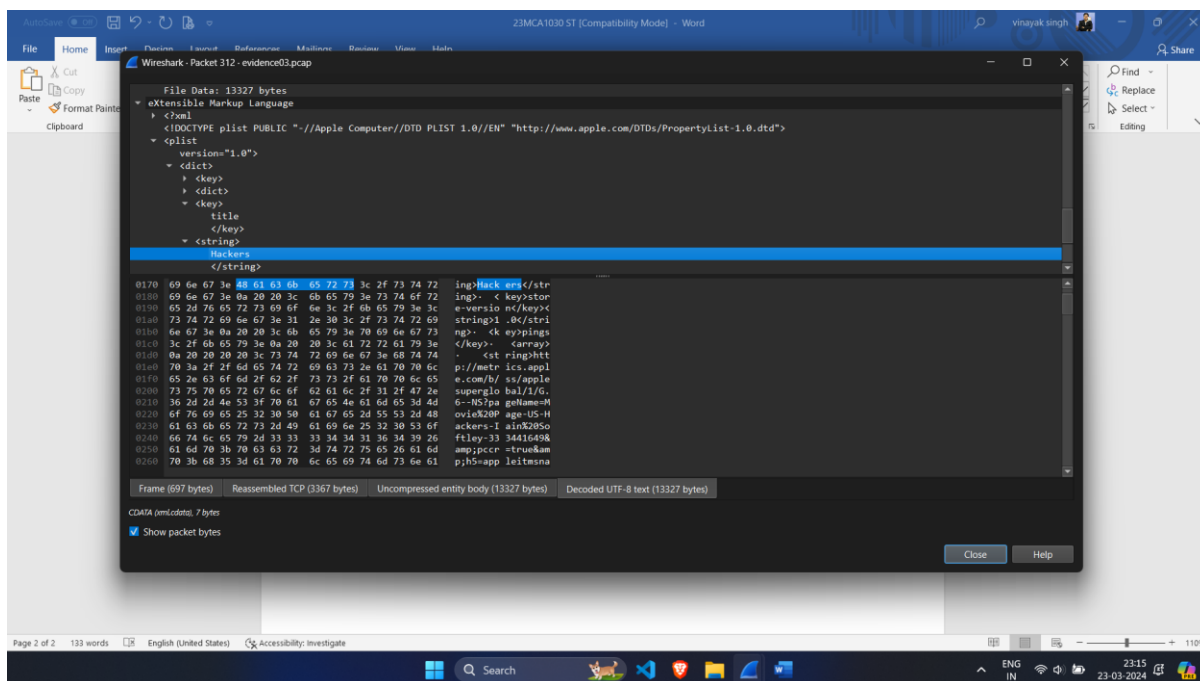
"/WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie"

```
p;artistTerm=Taylor%20Hackford</string>
  <key>url-page-type</key><string>list</string>
</dict>
<dict>
  <key>type</key><string>link</string>
  <key>title</key><string>Taylor Hackford</string>
  <key>url</key><string>http://ax.search.itunes.apple.com/WebObjects/MZSearch.woa/wa/a
p;artistTerm=Taylor%20Hackford</string>
  <key>url-page-type</key><string>list</string>
</dict>
</array>
</dict>
</plist>
GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=hack HTTP/1.1
Accept: */*
Accept-Language: en
Accept-Encoding: gzip, deflate
Cookie: s_vi=[CS]v1|259C176A85010C29-6000010D80115D7F[CE]
User-Agent: AppleTV/2.4
X-Apple-Store-Front: 143441-1,3
Connection: keep-alive
Host: ax.search.itunes.apple.com
```

4. What was the title of the first movie Ann clicked on?

**Ans:** Hacker

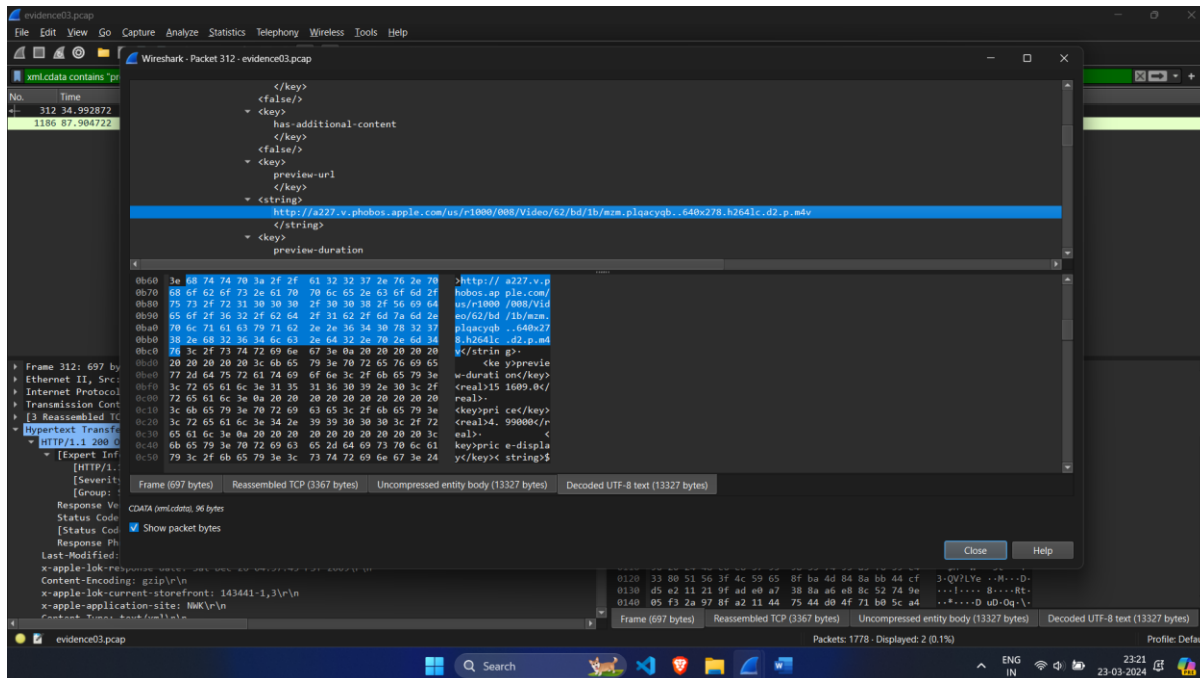
1. Search ip.dst == 66.235.132.121 and http.request.method == "GET"
2. xml.cdata contains "preview-url"
3. go to Extensible Markup Language XML and go to String



5. What was the full URL to the movie trailer (defined by “preview-url”)?

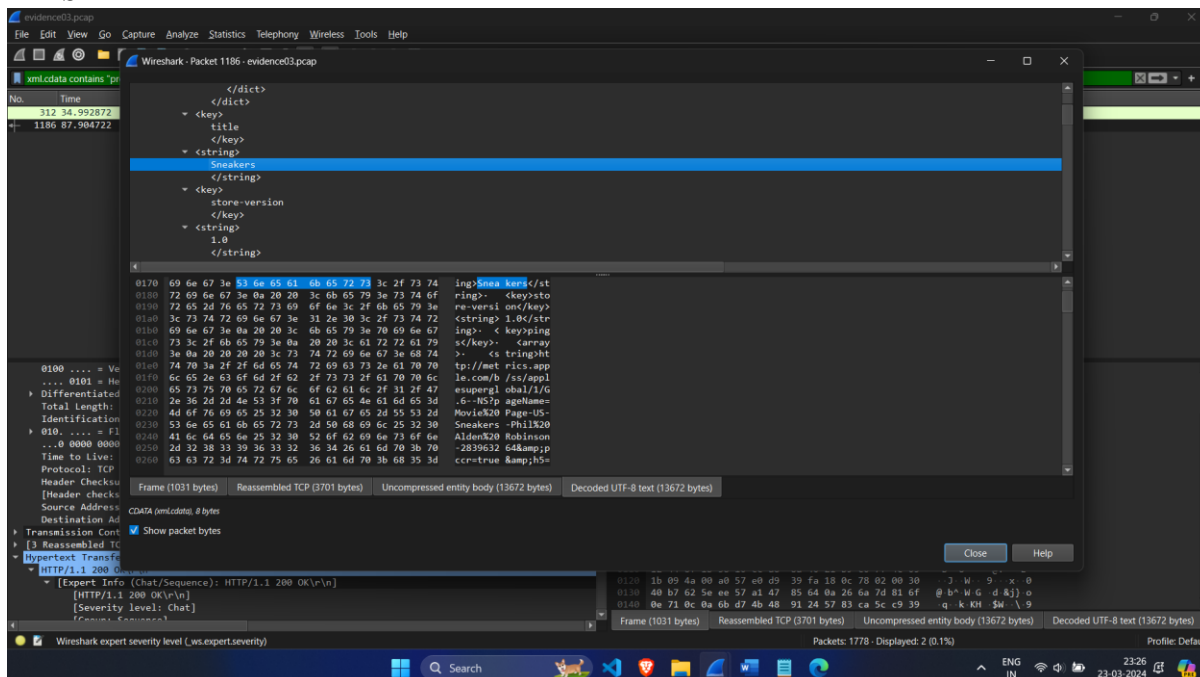
Ans:

<http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v>



6. What was the title of the second movie Ann clicked on?

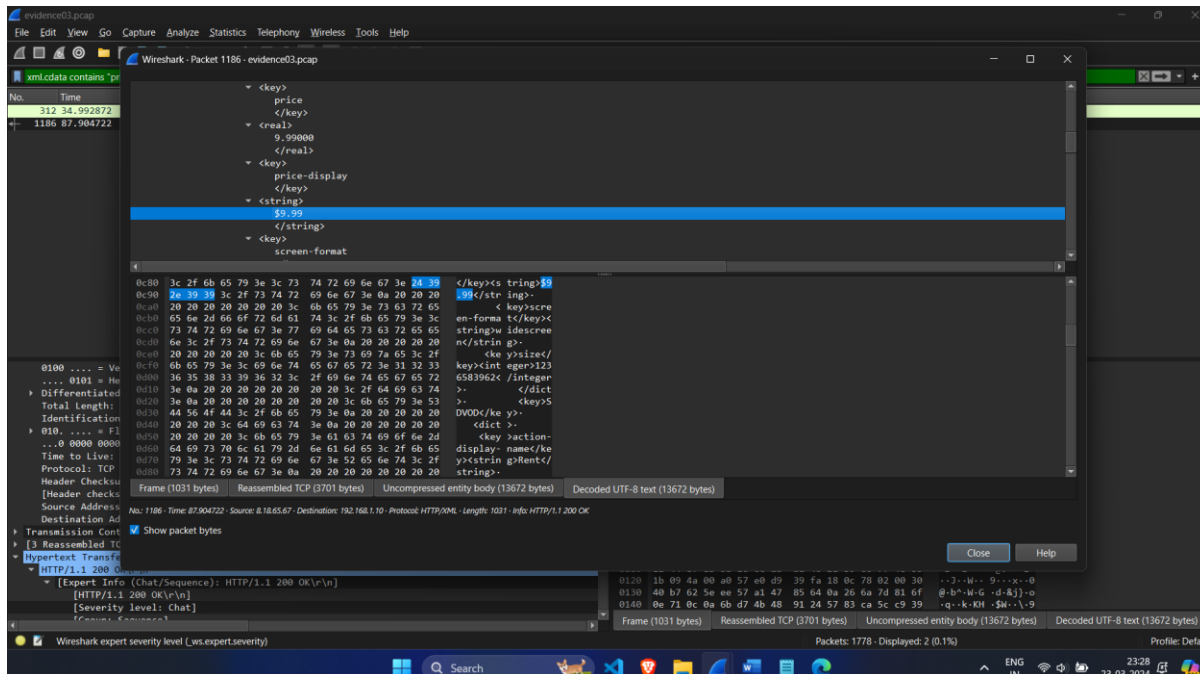
Ans: Sneakers



7. What was the price to buy it (defined by “price-display”)?

Ans: \$9.99

Search xml.cdata contains "price-display"



8. What was the last full term Ann searched for?

Ans: iknowyourewatchingme

1. http.request.uri contains "Search"
2. Follow Tcp Stream

