

작성자	박혜미
분석 일자	2024.05.12~2024.05.13
작성 일자	2024.05.13
분석 대상	evidence03.pcap
문서 버전	2.0
작성자 E-mail	mailto:parkm0708@naver.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부9

7. Reference 10

1. 문제

URL	https://forensicscontest.com/2009/12/28/anns-appletv
문제 내용	<p>Ann과 Mr. X는 새로운 운영 기반을 구축했습니다. 범죄인 인도 서류가 처리되기를 기다리는 동안 귀하와 귀하의 조사팀은 그녀의 활동을 은밀하게 모니터링합니다. 최근 Ann은 새로운 AppleTV를 구입하여 고정 IP 주소 192.168.1.10으로 구성했습니다. 다음은 그녀의 최근 활동이 포함된 <u>패킷 캡처입니다</u>.</p> <p>당신은 법의학 수사관입니다. 귀하의 임무는 Ann이 무엇을 검색했는지 알아내고, 관심 분야에 대한 프로필을 작성하고, 다음을 포함한 증거를 복구하는 것입니다.</p> <ol style="list-style-type: none"> 1. 앤의 AppleTV의 MAC 주소는 무엇입니까? 2. Ann의 AppleTV가 HTTP 요청에 사용한 User-Agent 문자열은 무엇입니까? 3. AppleTV에서 Ann의 처음 4개 검색어는 무엇이었습니까(모든 증분 검색이 포함됩니다)? 4. 앤이 클릭한 첫 번째 영화의 제목은 무엇이었나요? 5. 영화 예고편의 전체 URL("preview-url"로 정의됨)은 무엇입니까? 6. 앤이 클릭한 두 번째 영화의 제목은 무엇이었나요? 7. 그것을 사는 가격은 얼마였습니까("price-display"로 정의됨)? 8. Ann이 마지막으로 검색한 전체 용어는 무엇입니까?
문제 파일	 evidence03.pcap
문제 유형	네트워크 포렌식
난이도	2 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	https://www.wireshark.org/download.html	4.2.4

3. 환경

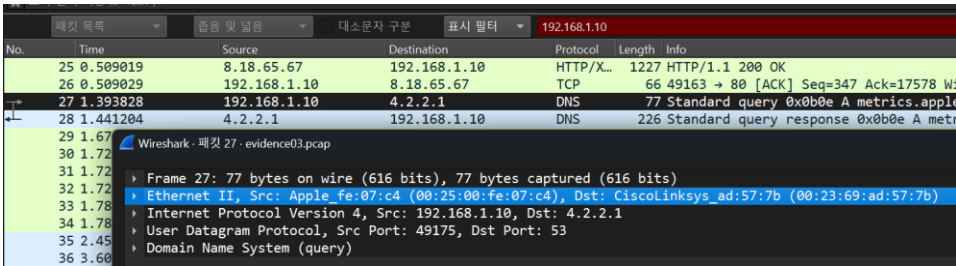
OS
Windows 11 Home

4. Write-Up

파일명	evidence03.pcap
용량	1.46MB
SHA256	740c49378a4302590cd88ecb768c148a6972afc44a606d123280be2d6a2e77d1
Timestamp	2024-05-13 12:57:59

시나리오가 긴데, 요약하자면 Ann 이 구매한 AppleTV 를 감시하는 것이다. 문제에서 알 수 있는 것은 IP 주소(192.168.1.10)와 패킷 정보이다.

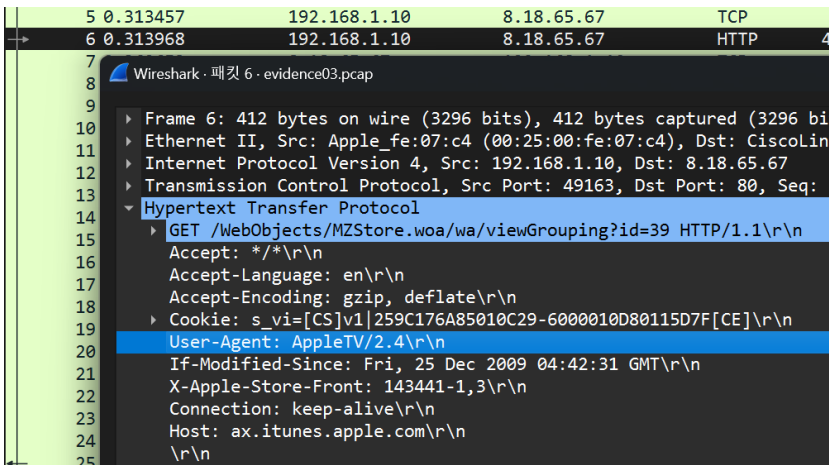
1. 앤의 AppleTV 의 MAC 주소는 무엇입니까?



[그림 1] Ann의 MAC 주소

문제에서 Ann 의 IP 주소를 알려주었으므로, 해당 IP 를 검색하면 MAC 주소를 알아낼 수 있다. Src(Source)가 바로 그 부분이며, 해당 **1 번 문제의 답은 00:25:00:fe:07:c4** 이다.

2. Ann 의 AppleTV 가 HTTP 요청에 사용한 User-Agent 문자열은 무엇입니까?



[그림 2] User-Agent

[WHS-2] .iso

Ann 의 IP 주소에서 HTTP 을 요청한 패킷을 자세히 보면 User-Agent 가 존재한다.

이때 wrWn 은 줄바꿈을 의미하는 것뿐이다. 또한 문자열을 찾으라고 했기 때문에 버전을 빼면 **2 번의 답은 AppleTV** 이다.

3. AppleTV 에서 Ann 의 처음 4 개 검색어는 무엇이었습니까(모든 증분 검색이 포함됩니까)?

여기서 incremental searches(증분 검색)이란 컴퓨터에서 사용자가 글자를 입력하는 도중에 계속적으로 해당하는 내용을 찾아주는 기능을 말한다. 보통 슬래시(/)를 사용한다고 한다.

```
TCP 66 49107 → 80 [ACK] Seq=1849 ACK=98478 Win=65535 Len=0 TSval=1093999810 TSecr=21408220
HTTP 385 GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=h HTTP/1.1
```

[그림 3] Ann의 1번 검색어 중 1자리

```
TCP 66 49107 → 80 [ACK] Seq=1849 ACK=98478 Win=65535 Len=0 TSval=1093999810 TSecr=21408220
HTTP 386 GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=ha HTTP/1.1
TCP 66 80 → 49165 [ACK] Seq=10999 Ack=640 Win=7504 Len=1368 TSval=2140825739 TSecr=1093999810
```

[그림 4] Ann의 1번 검색어 중 2자리

```
TCP 66 49107 → 80 [ACK] Seq=2409 ACK=12970 Win=65535 Len=0 TSval=1093999819 TSecr=21408220
HTTP 387 GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=hac HTTP/1.1
TCP 66 80 → 49165 [ACK] Seq=10999 Ack=640 Win=7504 Len=1368 TSval=2140825739 TSecr=1093999810
```

[그림 5] Ann의 1번 검색어 중 3자리

```
TCP 66 49107 → 80 [ACK] Seq=3077 ACK=16449 Win=65535 Len=0 TSval=1093999819 TSecr=21408220
HTTP 388 GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=hack HTTP/1.1
TCP 66 80 → 49165 [ACK] Seq=10999 Ack=640 Win=7504 Len=1368 TSval=2140825739 TSecr=1093999810
```

[그림 6] Ann의 1번 검색어 중 4자리

```
TCP 66 49107 → 80 [ACK] Seq=4 ACK=1 Win=65535 Len=0 TSval=1093999804 TSecr=21408220
HTTP 385 GET /WebObjects/MZSearch.woa/wa/incrementalSearch?media=movie&q=s HTTP/1.1
TCP 66 80 → 49171 [ACK] Seq=10999 Ack=640 Win=7504 Len=1368 TSval=2140821740 TSecr=1093999810
```

[그림 7] Ann의 2번 검색어 중 1자리

Ann 의 검색어를 찾기 위해 incremental 를 찾아보니, incrementalSearch?media=movie&q=다음에 문자열이 보인다. 계속해서 찾아본 결과 hack 에서 다음으로 s 를 검색한 것을 보아 Ann 은 가장 먼저 hack 을 검색한 듯하다. 따라서 **3 번의 답은 hack** 이다.

4. 앤이 클릭한 첫 번째 영화의 제목은 무엇이었나요?

```
1000001
/b/ss/applesuperglobal/1/G.6--NS?pageName=Movie%20Page-US-Hackers-Iain%20Softley-3
```

[그림 8] Hackers의 페이지에 방문

[WHS-2] .iso

3 번에서 media-movie 에서 검색한 것을 보아 해당 부분에서 영화를 찾기 위해 제목을 검색한 듯하다. 따라서 Wireshark 에 hack 을 검색하니 hack 이 아닌 Hackers 가 검색된 페이지에 방문했던 것을 확인할 수 있다.

5. 영화 예고편의 전체 URL("preview-url"로 정의됨)은 무엇입니까?

```
</raise/>
  <key>
    preview-url
  </key>
  <string>
    http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v
  </string>
```

[그림 9] preview-url

아마 해당 내용도 MAC 주소나 User-Agent 처럼 세부 내용에 있을 것으로 추측됨으로, 필터링으로 [패킷 자세한 정보]를 설정하고 preview-url 를 검색했더니 패킷이 하나 나온다. 내용을 보니 url 이 적혀져 있는 것을 확인할 수 있다. 따라서 5 번의 답은

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

6. 앤이 클릭한 두 번째 영화의 제목은 무엇이었나요?

```
66 [TCP Window Update] 491/6 → 80 [ACK] Seq=310 Ack=3/02 Win=65535 Len=0 TSva.
583 GET /b/ss/applesuperglobal/1/G.6--NS?pageName=Movie%20Page-US-Sneakers-Phi
107 GET /WebObjects/M7Store.wso/us/relatedItemsSelfGet?id=38&id=383863264&stor
```

[그림 10] Ann이 2번째로 검색한 영화 제목

해당 문제는 4 번 문제를 풀 때와 같은 방법으로 pageName 을 검색하여 Hackers 다음으로 방문한 사이트를 찾아보면 된다. 따라서 6 번의 답은 Sneakers 이다.

7. 그것을 사는 가격은 얼마였습니까("price-display"로 정의됨)?

```
</Field>
  <key>
    price-display
  </key>
  <string>
    $4.99
  </string>
```

[그림 11] Hackers의 가격

```
</real>
  <key>
    price-display
  </key>
  <string>
    $9.99
  </string>
```

[그림 12] Sneakers의 가격

해당 문제도 5 번처럼 세부 내용에 있을 것 같다. 따라서 필터링을 사용해 [패킷 자세한 정보]를 설정하고 price-display 을 검색하니 패킷이 나온다. 내용 안엔 price-display 의 내용이 들어있다. 하지만 가장 먼저 검색된 것은 Hackers 의 가격이므로 Sneakers 의 가격은 그 다음 패킷에 존재한다. 따라서 **7 번의 답은 \$9.99** 이다.

8. Ann 이 마지막으로 검색한 전체 용어는 무엇입니까?

```
%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Diknowyourewatchingme&pageName=Movies-Search%20
```

맨 마지막이라면 아래쪽에 있는 패킷에 있겠지 싶어 아래 정도에서 pageName 을 검색하였더니 1771 번 패킷이 가장 마지막 검색 용어였다. 해당 내용을 살펴보니 Ann 은 가장 마지막으로 **iknowyourwatchingme** 을 검색한 것을 볼 수 있다. **본인을 감시하는 것을 알고 있다** 는 소리이다. 그래서 Hackers 나 Sneakers(도둑, 숨기다)를 검색했던 것이다. 무섭다.



5. Flag

1 번: 00:25:00:fe:07:c4

2 번: AppleTV

3 번: hack

4 번: Hackers

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

6 번: Sneakers

7 번: \$9.99

8 번: iknowyourwatchingme

6. 별도 첨부

7. Reference

- incremental searches
 - https://ko.wikipedia.org/wiki/%EC%A6%9D%EB%B6%84_%EA%B2%80%EC%83%89