




# DATA EXTRACTION

Quick comparison between pcap carving tools  
and methods

# Case



- PCAP containing jpeg file
- Files transferred via unencrypted SMB
- Finding stream from pcap
- Recovering / reconstructing files

# Original picture



Monday, December 4, 2017 | Today's Paper | Video | 33°F | CAC 40 +0.65% ↑

World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Style Food Travel Magazine T Magazine Real Estate ALL



## Urus World Premiere

Today, live at 6PM (CET)

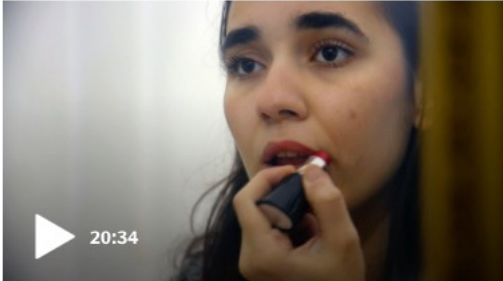
LAMBORGHINI.COM

### CVS Deal to Buy Aetna Could Reshape Health Industry

By MICHAEL J. de la MERCED and REED ABELSON 10:24 PM ET

- The \$69 billion deal would combine the drugstore giant with one of the United States' biggest health insurers.
- The companies touch most of the basic health services that people regularly use, but critics worry that customers

#### TIMES DOCUMENTARIES



20:34

Yousur Al-Hlou


### She Wants Independence. In Egypt, That Can Be Dangerous.

#### Opinion

### What's a Bigger Threat, 'Normalization' or Alarmism?

By IVAN KRASSTEV


Right-wing populists thrive in a culture of tense polarization. We shouldn't help them.



### A Fractured 2017

By ROGER COHEN

As the world lurches into a new year, peace feels fragile and the truth is blurred.




- Billy Bush: Yes, Donald Trump, You Said That

### To Stop North Korea, Act Like Israel

By NITSANA DARSHAN-LEITNER


Negotiations and sanctions haven't stopped the Kim regime. What about trying financial warfare?



### We Catalans Owe the World an Explanation

By ALBERT RIVERA

Coexistence and union are the best options to articulate a common project for Spain.



- Soil Power! The Dirty Way to a

- SHA256: 0781b0ad9687ed7b4f794b9431a2700a2ee036a3597441352b3fce79d0351825

# Tools

- Wireshark
  - Export packet bytes
- Foremost
  - Automated carving
- Tcpxtract
  - Automated carving
- 010 Hex Editor
  - Manual hex edit

# Wireshark

- Inspect pcap containing SMB traffic and transferred files
- Built-in file export can't find files inside pcap
- Locate file transfer and file size:

# JPEG

- Traffic from 192.168.198.1 to 192.168.198.131

30 0.896563	192.168.198.1	192.168.198.131	SMB2	1514 Write Request Len:131072 Off:0 File: Picture.jpeg
31 0.896564	192.168.198.1	192.168.198.131	TCP	1514 [Continuation to #30] 20642 → 445 [ACK] Seq=3600 Ack=2190 Win=2052 Len=1460
32 0.896564	192.168.198.1	192.168.198.131	TCP	1514 [Continuation to #30] 20642 → 445 [ACK] Seq=5060 Ack=2190 Win=2052 Len=1460
33 0.896566	192.168.198.1	192.168.198.131	TCP	1514 [Continuation to #30] 20642 → 445 [ACK] Seq=6520 Ack=2190 Win=2052 Len=1460

Time 30: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Internet II, Src: Vmware\_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware\_0b:6b:ea (00:0c:29:0b:6b:ea)

Internet Protocol Version 4, Src: 192.168.198.1, Dst: 192.168.198.131

Transmission Control Protocol, Src Port: 20642, Dst Port: 445, Seq: 2140, Ack: 2190, Len: 1460

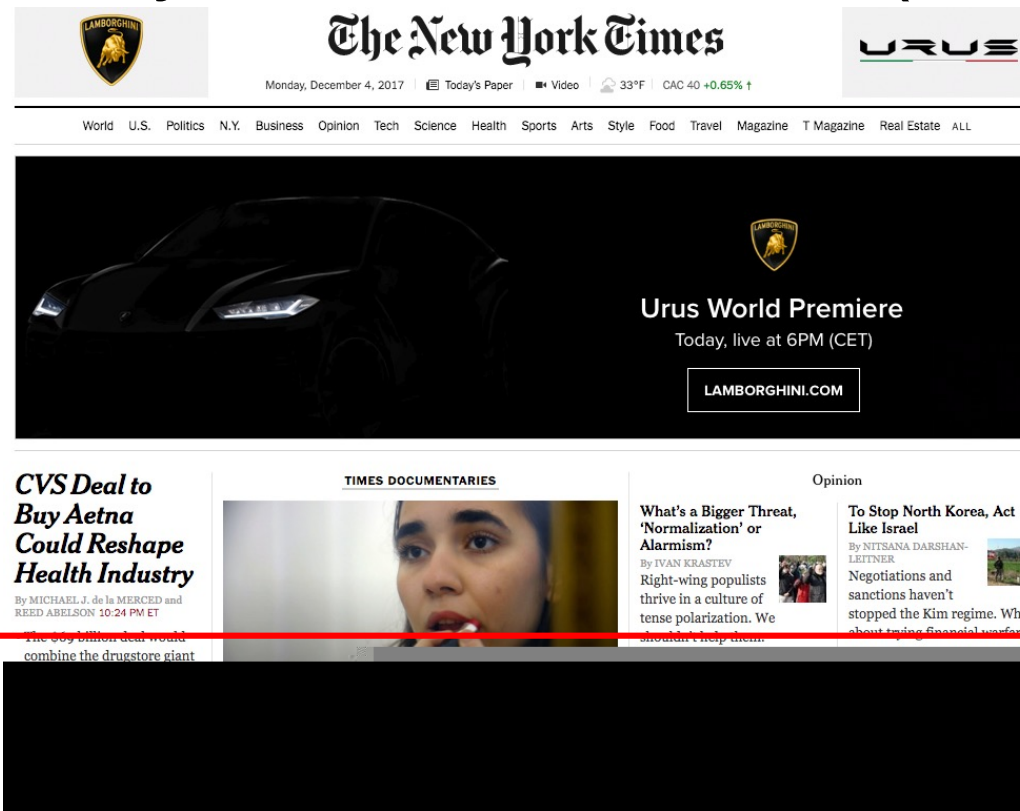
00 00 49 94 b0 27 00 00 00 00 00 00 00 00 00 00	..I...'.. .....
00 00 00 00 00 00 00 00 00 00 ff d8 ff e0 00 10	..... .....
4a 46 49 46 00 01 01 00 00 48 00 48 00 00 ff e1	JFIF.... .H.H....
00 4c 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08	..LExif.. MM.*....
00 01 87 69 00 04 00 00 00 01 00 00 00 1a 00 00	i

JPEG header

First packet and file length(not the actual file size. Transmission continues in another write request, packet 122 with file offset 131072, length 62331). Total length: 193403

# Foremost

- Able to carve file from extracted RAW
- Result (no flags):
  - JPEG partially found, size: 193519 (116 bytes +)



# Foremost

- PCAP input
- Result (no flags):
  - JPEG partially found, size: 202987 (9584 bytes +)

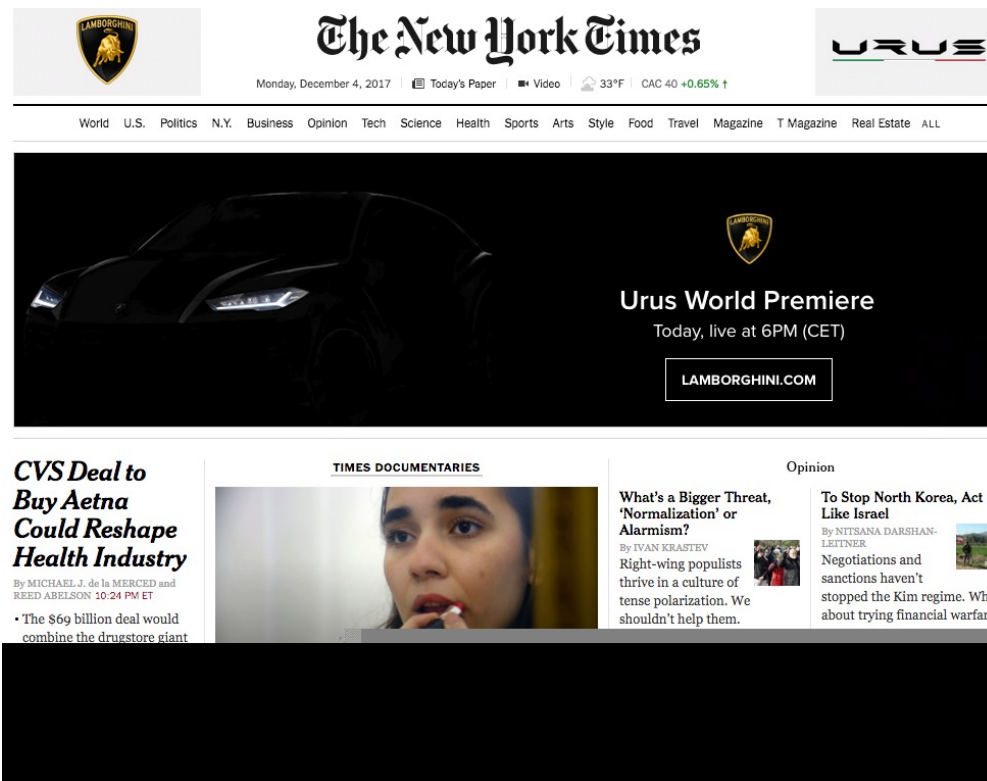


SHA256: 3b8afd9984d6f7aca5d236e74f301bc3ab056f451d846b16d64cf527169208a8



# Tcpxtract

- PCAP input only
- Result (no flags)
  - JPEG partially found, size: 193518 (115 bytes +)



SHA256: 5766aea56620fa781bcc97d0594cffbe0732387b9180e99ab12b87e40ed4e0b2

# Hex editor

- Extract RAW stream from Wireshark, import to hex editor
- Strip excess data before header and after trailer

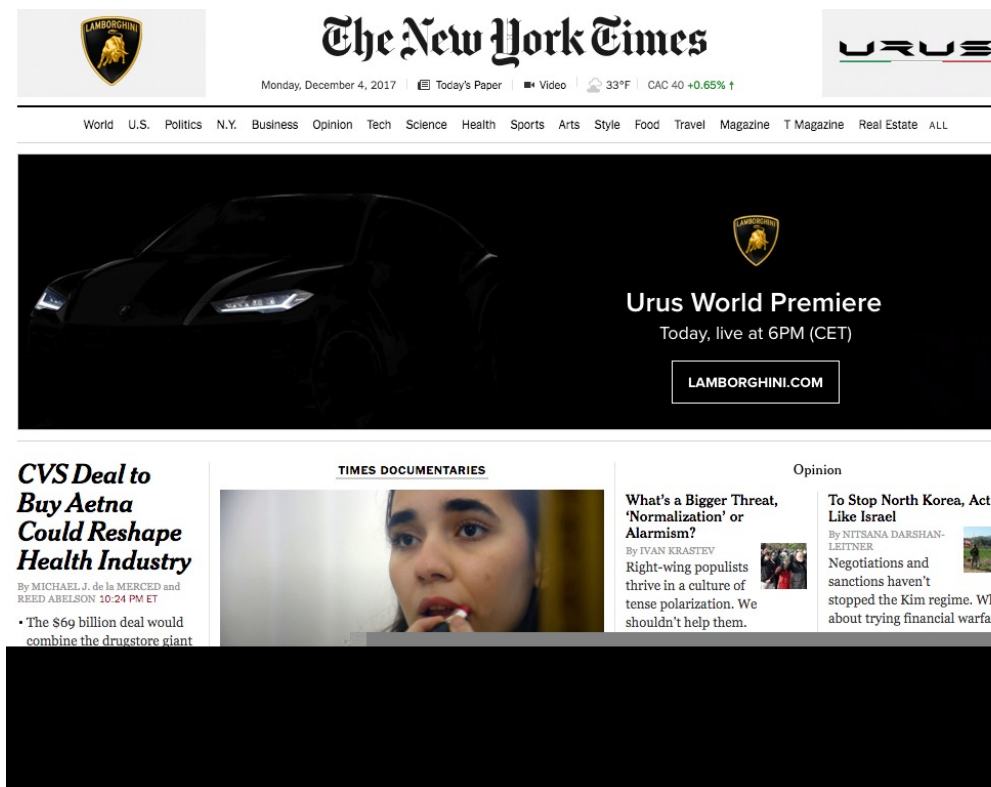
The image displays a hex editor window with two panels. The top panel shows a range of memory addresses from 0820h to 0920h. The bottom panel shows a range from 2:FC90h to 2:FD00h. Annotations with arrows point to specific data regions:

- Cleartext NW traffic:** Points to the SMB header at offset 0860h, where the bytes `53 4D 42 40` are highlighted with a yellow box.
- JPEG header:** Points to the start of the JPEG data at offset 08D0h, where the bytes `D8 FF E0` are highlighted with a red box.
- JPEG trailer:** Points to the end of the JPEG data at offset 2:FCB0h, where the bytes `FF D9` are highlighted with a red box.

The hex editor shows the raw bytes in hexadecimal and their corresponding ASCII representation. The ASCII column contains various characters, including control characters and printable text like "SMB@" and "JFIF".

# Hex editor

- Saved as .jpeg
  - Picture partially recovered, size 193519 (116 bytes +)



SHA256: ac695c60eff5aa75b63115792f25083e4430cd964324de1a00e1109d615dc330

!Matches with Foremost RAW extract!

# Finding differences

- Skip Foremost PCAP results...
- Locate 116 excess bytes from tcpxtract output file with hex editor

1:FFF0h:	D0 C6 8D 76 B8 F7 A9 61 BA C1 E6 B9 C7 9F 9E 4D	DE.v -@a°Áæ³ÇŸŽM
2:0000h:	00 00 F3 EB FE 53 4D 42 40 00 01 00 00 00 00 00	...ôëpSMB@.....
2:0010h:	09 00 00 00 30 00 00 00 00 00 00 00 77 00 00 00	....0.....w...
2:0020h:	00 00 00 00 FF FE 00 00 B8 96 9C 68 29 75 AD C6	....ÿþ.,-œh)u- E
2:0030h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
2:0040h:	00 00 00 00 31 00 70 00 7B F3 00 00 00 00 02 00	....l.p.{ó.....
2:0050h:	00 00 00 00 F6 BD 83 2B 00 00 00 00 49 94 B0 27	....ö¼f+....I"°'
2:0060h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
2:0070h:	00 00 00 00 49 04 FE 86 93 63 B9 D9 2D C8 2B 8F	....I.p+"c¹Û-Ê+.
2:0080h:	5A BA 1A 3D 80 1E 0F B1 AE 3D 6E 8E 07 B5 5D 3A	Z°. =€...±@=nŽ.µ]:

116 bytes, starting from 2:000h:

NW traffic

# Result

- Save as .jpeg

The screenshot shows the front page of The New York Times website. At the top, the masthead reads "The New York Times" in its signature font. To the left is the Lamborghini logo, and to the right is the Urus logo. Below the masthead, a navigation bar lists various sections: World, U.S., Politics, N.Y., Business, Opinion, Tech, Science, Health, Sports, Arts, Style, Food, Travel, Magazine, T Magazine, Real Estate, and ALL. The main banner is a large black image of a Lamborghini Urus with the text "Urus World Premiere" and "Today, live at 6PM (CET)". Below this is a button that says "LAMBORGHINI.COM".

Below the banner, the page is divided into several sections:

- CVS Deal to Buy Aetna Could Reshape Health Industry**  
By MICHAEL J. de la MERCED and REED ABELSON 10:24 PM ET  
• The \$69 billion deal would combine the drugstore giant with one of the United States' biggest health insurers.  
• The companies touch most of the basic health services that people regularly use, but critics worry that customers
- TIMES DOCUMENTARIES**  
A video player showing a woman with the title "She Wants Independence. In Egypt, That Can Be Dangerous." and a duration of 20:34.
- Opinion**
  - What's a Bigger Threat, 'Normalization' or Alarmism?**  
By IVAN KRASSTEV  
Right-wing populists thrive in a culture of tense polarization. We shouldn't help them.
  - A Fractured 2017**  
By ROGER COHEN  
As the world lurches into a new year, peace feels fragile and the truth is blurred.
  - To Stop North Korea, Act Like Israel**  
By NITTSANA DARSHAN-LETTNER  
Negotiations and sanctions haven't stopped the Kim regime. What about trying financial warfare?
  - We Catalans Owe the World an Explanation**  
By ALBERT RIVERA  
Coexistence and union are the best options to articulate a common project for Spain.
  - Billy Bush: Yes, Donald Trump, You Said That**
  - Soil Power! The Dirty Way to a**

SHA256: 0781b0ad9687ed7b4f794b9431a2700a2ee036a3597441352b3fce79d0351825

Matches with original:

SHA256: 0781b0ad9687ed7b4f794b9431a2700a2ee036a3597441352b3fce79d0351825