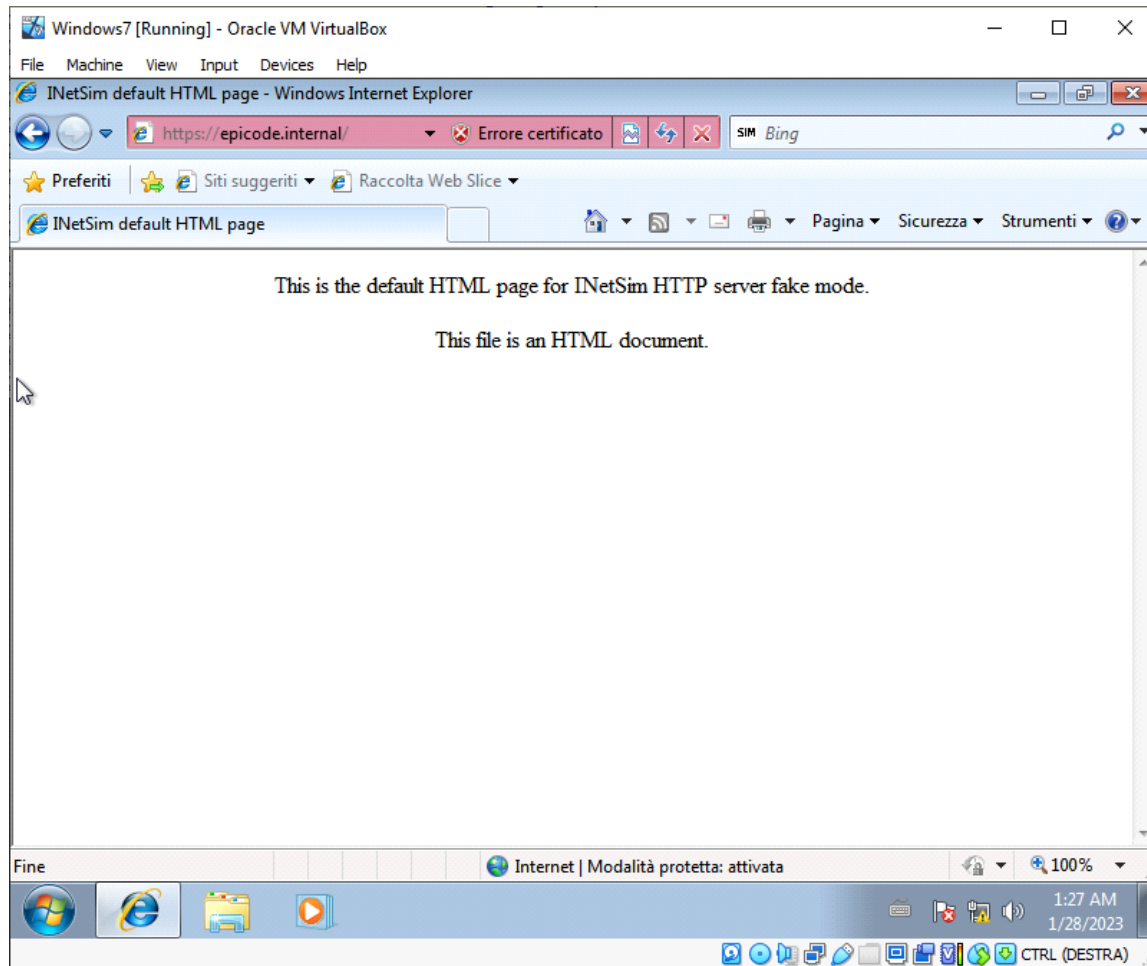
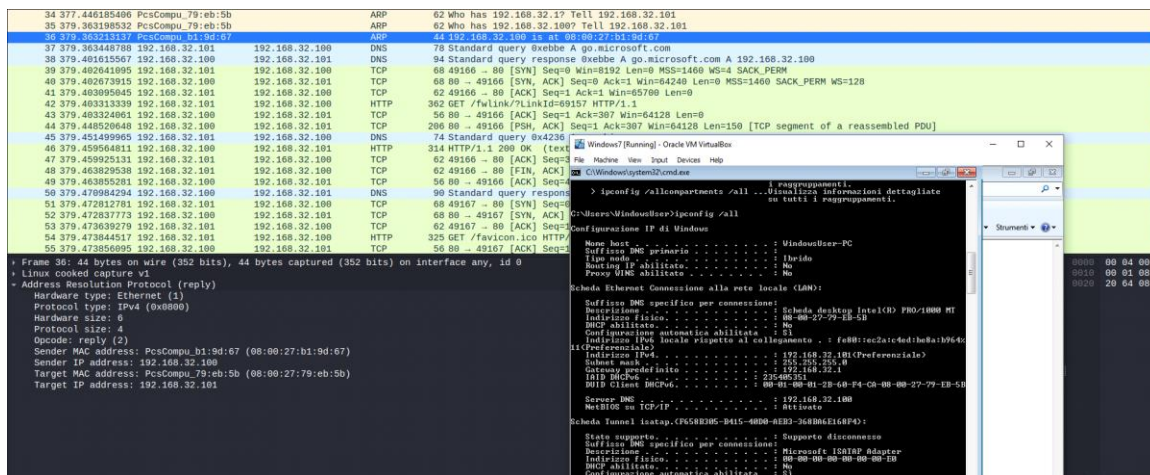
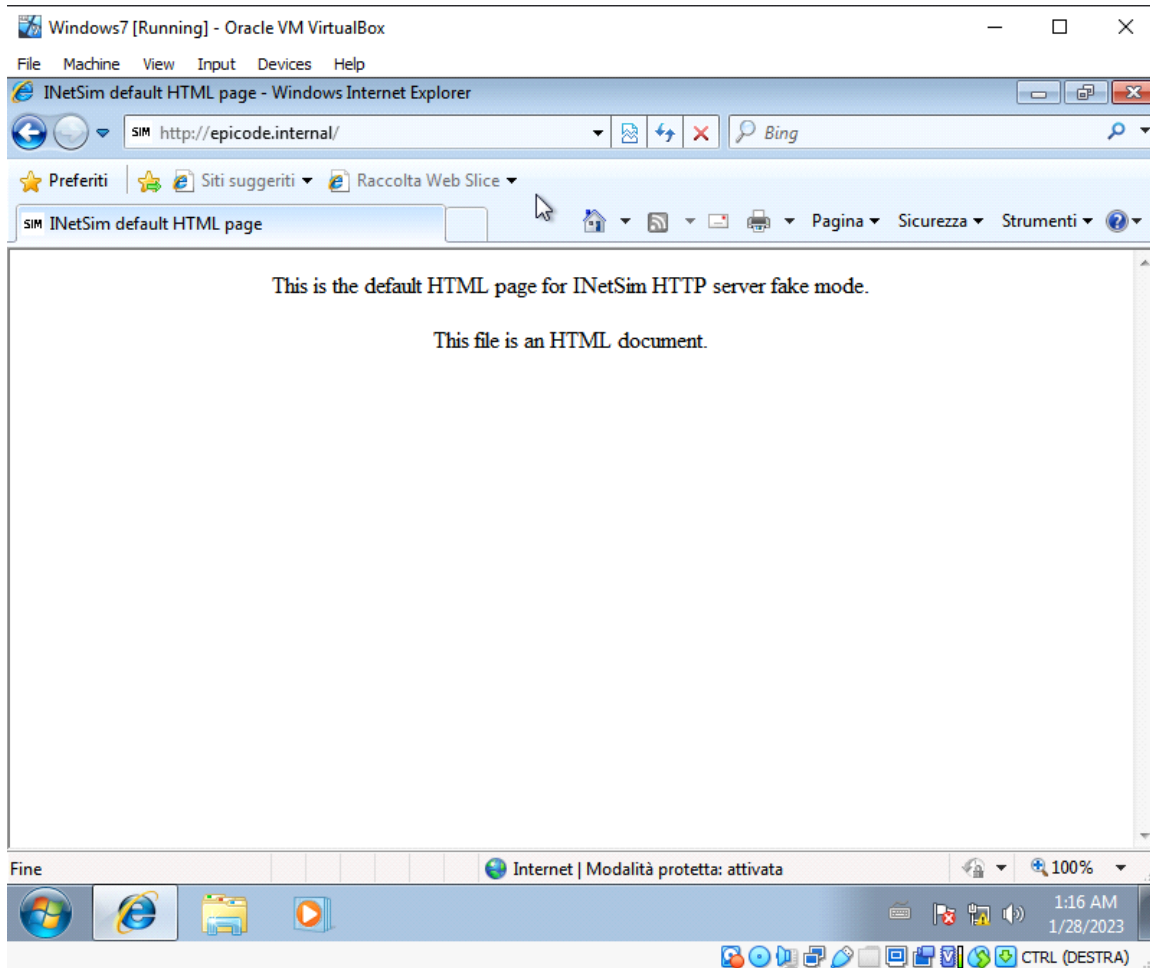


Richiesta sito in https



821	767.535883853	192.168.32.101	192.168.32.100	TCP	68 49207 -> 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM	
822	767.535884869	192.168.32.100	192.168.32.101	TCP	80 80 -> 49207 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
823	767.536411788	192.168.32.101	192.168.32.100	TCP	62 49207 -> 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
824	767.536850457	192.168.32.101	192.168.32.100	HTTP	273 GET /msdownload/update/v3/static/trusted/en/authrootstl.cab HTTP/1.1	
825	767.536884680	192.168.32.100	192.168.32.101	TCP	56 80 -> 49207 [ACK] Seq=1 Ack=218 Win=64128 Len=0	
826	767.621665777	192.168.32.100	192.168.32.101	TCP	206 80 -> 49207 [PSH, ACK] Seq=1 Ack=218 Win=64128 Len=150 [TCP segment of a reassembled PDU]	
827	767.627738290	192.168.32.101	192.168.32.100	HTTP	314 HTTP/1.1 200 OK (text/html)	
828	767.628087043	192.168.32.101	192.168.32.100	TCP	62 49207 -> 80 [ACK] Seq=218 Ack=410 Win=65280 Len=0	
829	767.629055157	192.168.32.101	192.168.32.100	TCP	62 49207 -> 80 [FIN, ACK] Seq=218 Ack=410 Win=65280 Len=0	
830	767.629071429	192.168.32.100	192.168.32.101	TCP	56 80 -> 49207 [ACK] Seq=410 Ack=219 Win=64128 Len=0	
831	768.610905577	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
832	768.610905588	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
833	768.611266311	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
834	771.096710470	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
835	771.047308097	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
836	772.598094430	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
837	773.369116111	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
838	774.114298849	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
839	775.114483592	PcsCompu_79:eb:5b	PcsCompu_79:eb:5b	ARP	62 Who has 192.168.32.17 Tell 192.168.32.101	
840	776.805156550	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
841	777.553653790	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
842	778.304311530	192.168.32.101	192.168.32.255	NBNS	94 Name query NB WPAD<00>	
+ Frame 831: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0						
- Linux cooked capture v1						
Packet type: Broadcast (1)						
Link-layer address type: Ethernet (1)						
Link-layer address length: 6						
Source: PcsCompu_79:eb:5b (08:00:27:79:eb:5b)						
Unused: 3239						
Protocol: ARP (0x0008)						
Padding: 00000000000000000000000000000000						
Trailer: 0000						
- Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0008)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: PcsCompu_79:eb:5b (08:00:27:79:eb:5b)						
Sender IP address: 192.168.32.101						
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.32.1						

Richiesta sito in http



Quando proviamo a connetterci ad un sito con il protocollo https i nostri dati vengono cifrati per poi essere decifrati dal ricevente, quindi quando intercettiamo questo tipo di pacchetti non otteniamo alcuna informazione riguardo al mittente perchè pur avendo intercettato i dati non possiamo leggerli.

Quando il sito ha un protocollo http invece i dati non vengono cifrati quindi chiunque intercetti questo tipo di pacchetti può ottenere tutte le informazioni contenute mettendo a rischio la privacy e la

sicurezza del mittente.