Digital Forensics

Digital Forensics

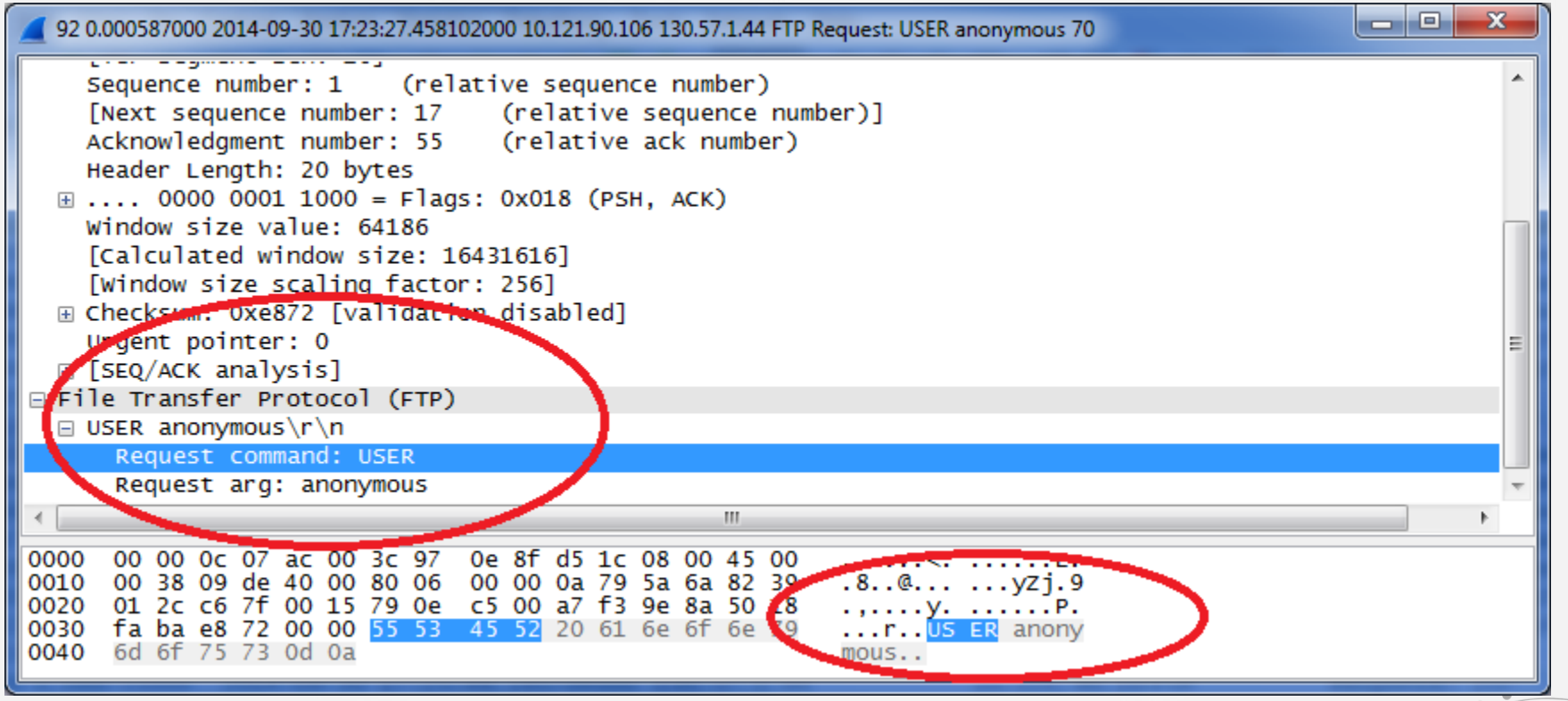
- What is “digital forensics”?
- Using Wireshark for forensics
  - Capturing sensitive data
  - Capturing cleartext (data, credentials, etc.)
  - Network mapping (IP addressing, DNS, etc.)
- Wireshark and privacy
  - Get permission!

Digital Forensics

Filter: ftp | Expression... | Clear | Apply | Save

No.	Time	UTC	Source	Destination	Protocol	Info
91	0.000000000	2014-09-30 17:23:27.457515000	130.57.1.44	10.121.90.10	FTP	Response: 220 Welcome to ftp.novell.com, powered by SUSE Linux
92	0.000587000	2014-09-30 17:23:27.458102000	10.121.90.106	130.57.1.44	FTP	Request: USER anonymous
95	0.089959000	2014-09-30 17:23:27.548061000	130.57.1.44	10.121.90.10	FTP	Response: 331 Anonymous login ok, send your complete email address as
96	0.000547000	2014-09-30 17:23:27.548608000	10.121.90.106	130.57.1.44	FTP	Request: PASS anon@localhost
98	0.090772000	2014-09-30 17:23:27.639380000	130.57.1.44	10.121.90.10	FTP	Response: 230 Anonymous access granted, restrictions apply
99	0.001111000	2014-09-30 17:23:27.640491000	10.121.90.106	130.57.1.44	FTP	Request: OPTS UTF8 ON
104	0.087976000	2014-09-30 17:23:27.728467000	130.57.1.44	10.121.90.10	FTP	Response: 200 UTF8 set to on
105	0.001952000	2014-09-30 17:23:27.730419000	10.121.90.106	130.57.1.44	FTP	Request: PWD
112	0.098107000	2014-09-30 17:23:27.828526000	130.57.1.44	10.121.90.10	FTP	Response: 257 "/" is the current directory
543	18.097594000	2014-09-30 17:23:45.926120000	130.57.1.44	10.121.90.10	FTP	Response: 220 Welcome to ftp.novell.com, powered by SUSE Linux
544	0.000751000	2014-09-30 17:23:45.926871000	10.121.90.106	130.57.1.44	FTP	Request: USER anonymous
546	0.094911000	2014-09-30 17:23:46.021782000	130.57.1.44	10.121.90.10	FTP	Response: 331 Anonymous login ok, send your complete email address as
547	0.001467000	2014-09-30 17:23:46.023249000	10.121.90.106	130.57.1.44	FTP	Request: PASS anon@localhost
549	0.090875000	2014-09-30 17:23:46.114124000	130.57.1.44	10.121.90.10	FTP	Response: 230 Anonymous access granted, restrictions apply
550	0.000522000	2014-09-30 17:23:46.114646000	10.121.90.106	130.57.1.44	FTP	Request: OPTS UTF8 ON
552	0.090460000	2014-09-30 17:23:46.205106000	130.57.1.44	10.121.90.10	FTP	Response: 200 UTF8 set to on
553	0.001843000	2014-09-30 17:23:46.206949000	10.121.90.106	130.57.1.44	FTP	Request: PWD
556	0.088755000	2014-09-30 17:23:46.295704000	130.57.1.44	10.121.90.10	FTP	Response: 257 "/" is the current directory

Digital Forensics



Questions?